Anexa 18
H.S. nr: 29/17.06.2013

ROMÂNIA
MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal 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 utilizare a Resurselor Informatice şi de Comunicații

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de utilizare a Resurselor Informatice şi de Comunicaţii

Introducere

În acord cu prevederile Politicii de Securitate, Resursele Informatice şi de Comunicaţii (RIC) sunt bunuri strategice ale Universităţii din Oradea care trebuiesc administrate ca resurse ale statului român. Acest regulament este stabilit astfel încât:

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

Audienta

Regulamentul de Utilizare a Resurselor Informatice şi de Comunicaţii al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

Confidenţialitate

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 personalul responsabil cu securitatea RIC ale Universităţii din Oradea, în condiţiile prevăzute de lege.

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*

[1] Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof. univ. dr. SORIN CURILĂ

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.
- *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 utilizare a Resurselor Informatice şi de Comunicaţii

A. Utilizarea permanentă a Resurselor Informatice şi de Comunicaţii

1. Utilizarea Resurselor Informatice şi de Comunicaţii (RIC) se face numai în interes de serviciu.

2. Utilizatorii trebuie să anunţe Serviciul Management Integrat IT atât despre orice problemă/breşă în sistemul de securitate din cadrul Universităţii din Oradea, cât şi despre orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.

3. Prin acţiunile lor, utilizatorii 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.

4. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.

5. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: *Smartcard*) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.

6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală si a dreptului de autor (*copyright*).

7. 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.

8. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele sistemelor ce alcătuiesc 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.

---

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte, Prof.univ.dr. SORIN CURILĂ

9. 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 UO nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.

10. RIC ale Universităţii din Oradea nu trebuie să fie folosite pentru beneficiul personal.

11. 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).

12. 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.

13. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la Resursele Informatice şi de Comunicaţii ale Universităţii.

14. Utilizatorii care au acces la RIC ale Universităţii din Oradea au obligaţia de a purta acte şi sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile instituţiei.

15. Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activităţile desfăşurate prin intermediul sau folosind RIC ale Universităţii din Oradea.

16. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Universităţii din Oradea folosind RIC.

17. 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.

18. În scopul administrării şi pentru asigurarea securităţii RIC 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 în limitele şi conform procedurilor prevăzute de legislaţia în vigoare.

B. Utilizarea ocazională a Resurselor Informatice şi de Comunicaţii

În anumite situaţii este permisă utilizarea ocazională a RIC. În aceste situaţii se aplică următoarele restricţii:

- utilizarea personală ocazională a serviciilor de poştă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane;
- utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Universitate;
- utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.

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;

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 27.06.2013
Președinte: Prof.univ.dr. SORIN CURILA

- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. ~~Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.~~
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Confidențialitatea Serviciilor Informatice şi de Comunicații

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

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Regulamente privind Confidențialitatea Serviciilor Informatice şi de Comunicații

Introducere

Regulamentele de Confidențialitate sunt mecanisme utilizate pentru a stabili limite pentru utilizatorii RIC. Confidențialitatea informației este asigurată în cadrul RIC al Universității din Oradea în condițiile legislației în vigoare. ~~Utilizatorii interni nu ar trebui să se aştepte la confidenţialitate în ceea ce priveşte utilizarea sistemului RIC.~~ Utilizatorii externi ar trebui să se aştepte la confidențialitate totală, cu excepția cazului în care se suspectează un delict cu privire la sistemul RIC.

Scopul

Scopul Regulamentului privind Confidențialitatea Serviciilor Informatice şi de Comunicații ale Universității din Oradea este acela de a comunica în mod clar utilizatorilor prevederile referitoare la confidențialitatea datelor stocate în sistemul RIC.

Audienta

Regulamentul privind Confidențialitatea Serviciilor Informatice şi de Comunicații al Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității din Oradea.

Confidenţialitate

Fişierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia şi sub controlul Universității din Oradea, cad sub incidența reglementărilor legale privind proprietatea intelectuală. ~~sunt proprietatea Universității în condițiile legilor în vigoare~~.

Definiții

- *Resurse Informatice şi de Comunicații* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi 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 şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- *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.
- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de orice 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.
- *Server Web*: un sistem de calcul care distribuie în mod public sau diferențiat informații folosind protocolul HTTP.
- *Pagină web*: Un document în spațiul World Wide Web (WWW). Fiecare pagină web este identificată printr-un URL (*Uniform Resource Locator*).

Regulament privind Confidențialitatea Serviciilor Informatice și de Comunicații

- Fișierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia și sub controlul Universității din Oradea ~~nu~~ sunt confidențiale și pot fi accesate ~~oricând~~ de către angajații autorizați din cadrul Serviciului Management Integrat IT, Departamente / Departamente și Facultăți în condițiile prevăzute de lege. ~~fără înștiințarea utilizatorului conform Regulamentului de Acces Administrativ~~.
- În scopul administrării RIC și pentru asigurarea securității RIC personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor în limitele și conform procedurilor prevăzute de legislația în vigoare.
- Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universității, orice incident de posibilă întrebuințare greșită sau încălcare a acestui regulament (prin contactarea CIC).
- Un mare număr de utilizatori (inclusiv studenți), pot accesa informații din exteriorul sistemului de comunicații al Universității. În aceste condiții este obligatorie păstrarea confidențialității informațiilor transmise din exteriorul RIC și a informațiilor obținute din interior.
- Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universității pentru care nu au autorizație sau consimțământ explicit.
- Nici un utilizator al sistemului RIC al Universității nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului RIC. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Universitatea.
- Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

confidențiale ale Universității se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

Regulament pentru Accesul Publicului la Informații

Cookie-uri: Un "cookie" este un fișier care conține informație plasată de către un server web pe un calculator al utilizatorului. De obicei, aceste fișiere sunt utilizate pentru a facilita accesul la informația oferită de sit-ul web. Orice informație pe care serverele web ale Universității din Oradea o pot stoca în cookie-uri este utilizată numai în interiorul UO. Informația din cookie-uri nu este utilizată pentru a dezvălui, către terți, informații despre vizitator decât în cazul în care Universității din Oradea i se cere în mod legal să facă acest lucru în conformitate cu legile în vigoare sau alte proceduri legale.

Jurnale și Monitorizare: Universitatea din Oradea păstrează fișierele cu înregistrări ale tuturor accesărilor sit-urilor sale și de asemenea monitorizează traficul din rețea în scopul administrării sit-urilor. Această informație este utilizată pentru a ajuta la diagnosticarea eventualelor probleme și pentru a realiza alte sarcini administrative. Uneltele de analiză a jurnalelor sunt de asemenea utilizate pentru statistici în scopul determinării informației cu un grad ridicat de interes pentru utilizatori sau vizitatori. Informațiile incluse în aceste fișiere sunt:

- *numele sistemului:* numele sistemului și/sau adresa IP a calculatorului care cere accesarea sit-ului.
- *Agent-Utilizator:* tipul browser-ului, versiunea, și sistemul de operare al calculatorului care cere accesarea site-ului
- *Referință:* pagina web de unde a venit utilizatorul.
- *Data sistemului:* data și ora accesării.
- *Cerere completă:* cererea exactă făcută de utilizator.
- *Stare:* codul de stare returnat de server, ex: "*file not found*" (nu a găsit fișierul).
- *Mărimea conținutului:* lungimea, în bytes (octeți), a fișierului trimis utilizatorului.
- *Metodă:* metoda cererii folosită de către browser (ex.: post, get).
- *Uniform Resource Identifier (URI):* adresa unei anumite resurse cerute.
- *Șir de interogare din URI:* orice după un semn de întrebare în cadrul unui URI. De exemplu, dacă a fost cerut un cuvând cheie de căutare, acel cuvânt cheie va apare în șirul interogării.
- *Protocol:* protocolul tehnic și versiunea utilizată, de ex.: http 1.0, ftp, etc.

Informația de mai sus nu va fi folosită pe nici o cale care ar putea dezvălui informație de identificare personală unei persoane din exteriorul Universității din Oradea, decât dacă se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale. De asemenea este interzisă utilizarea informației de către administratorii sistemului IT în alte scopuri decât cele privind administrarea sistemului, respectiv de prevenire a activităților ilegale sau imorale.

Informație din mesaje electronice sau formulare: Dacă un vizitator trimite un mesaj electronic Universității din Oradea sau completează un formular web cu o întrebare sau comentariu ce conține informație de identificare personală, acea informație va fi utilizată numai pentru a răspunde cererii și pentru a analiza intențiile. Mesajul poate fi redirectat la altă persoană care este calificată să răspundă cererii. Astfel de informații nu vor fi folosite pe nici o cale prin care s-ar dezvălui informație de identificare personală terților, cu excepția cazului în care Universității i se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale.

Legături: Acest sit poate conține legături la alte sit-uri. Universitatea din Oradea nu este răspunzătoare de politicile de securitate sau conținutul acestor sit-uri.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Contact: Dacă aveți întrebări în legătură cu această declarație sau utilizarea acestui site vă rugăm să ne contactați.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. ~~Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor~~.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Rețeaua de Comunicații

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

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)

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 12.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității 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 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 la Rețeaua de Comunicații

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

2. Departamentele / Centrele şi Facultățile trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Universității. 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 Universității nu se pot conecta la altă rețea.

6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în nici un fel, pe nici o cale. Nu este permisă instalarea de conexiuni de rețea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăților / Centrelor şi a Departamentelor de către Serviciul Management Integrat IT.

8. Sistemele computerizate din afara Universității care necesită conectare la rețea trebuie să se conformeze cu standardele rețelei interne ale Universității.

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 Universității nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectați la rețeaua Universității.

10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, 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 rețelei Universității cu alte rețele sunt realizate exclusiv de către Serviciul de Management Integrat IT.

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

[3] Trebuie reglementat acest aspect

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Administrativ

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Regulament de Acces Administrativ

Introducere

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

Scopul

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

Audienta

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

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* □ndeplineşte 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.

---

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 12.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității 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 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 şi 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 sa aibă instrucțiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare Departament / Centru sau Facultate şi vor fi incluse în fişa postului.
3. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi 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 desfăşoară.
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 şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi 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 şters atunci când nu mai este necesar.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi de Comunicații.

Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Referințe

1. http://dcd.uaic.ro/?page_id=90

APROBAT ÎN ŞEDINȚA DE SENAT DIN DATA DE 27.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

2. http://www.uaiasi.ro/diacd/
3. http://www.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Administraţie (CA)	**Senatul Universităţii din Oradea (SUO)**
Hotărîrea CA nr.	Hotărîrea SUO nr.
Data:	Data:

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

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*

[1] Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

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.
- 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.

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal 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 tratare a incidentelor de securitate

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de tratare a incidentelor de securitate

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

Acest document descrie cerinţele şi regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate. Acestea includ (dar nu sunt limitate la): detectarea programelor de tip virus, vierme informatic etc., folosirea neautorizată a conturilor de acces şi a calculatoarelor în sine, precum şi reclamaţiile privind folosirea improprie a RIC după cum este subliniat în regulamente.

Audienta

Regulamentul privind Tratarea Incidentelor de Securitate se aplică nediscriminatoriu tuturor persoanelor care folosesc orice componentă a 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)

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității 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 acțiunii respective.
- *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii Universității din Oradea în baza unui contract comercial sau de colaborare.
- *Echipă de Răspuns la Incidentele de Securitate a RIC* (ERIS): personalul responsabil de acțiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate.
- *Virus*: Un program care se auto-ataşează la un fişier executabil sau la o aplicație vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe *Microsoft Office* (*Word, Excel, PowerPoint*) sau alte programe care permit utilizatorului să genereze macro-uri.
- *Vierme*: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul rețelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o rețea de calculatoare, folosind resursele sau calculatoarele neutilizate din rețea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o amenințare la adresa securității datorită faptului că folosesc rețeaua pentru a se împrăştia, împotriva voinței proprietarilor de sisteme de calcul, cauzând astfel nefuncționarea sau funcționarea defectuoasă a rețelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferența constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.
- *Cal troian*: de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.
- *Incident de Securitate*: În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrității şi/sau confidențialității informației de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informațiilor, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiința sau intenția utilizatorului.

REGULAMENT de tratare a incidentelor de securitate

1. În cazul incidentelor de securitate din Universitatea din Oradea, membrii Serviciului Management Integrat IT au funcții şi responsabilități predefinite care pot fi prioritare îndatoririlor obişnuite.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

2. Ori de câte ori un incident de securitate este suspectat sau confirmat (exemple: virus, vierme, descoperirea unor activități suspecte, informații modificate etc.), trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.

3. Serviciul Management Integrat IT este responsabilă cu înştiințarea şi coordonarea pentru tratarea incidentului.

4. Serviciul Management Integrat IT este responsabilă cu strângerea dovezilor fizice şi electronice ce vor face parte din documentația pentru tratarea incidentului.

5. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităților acolo unde este cazul.

6. Serviciul Management Integrat IT va stabili conținutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informații.

7. Serviciul Management Integrat IT trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informațiile utile pentru eliminarea sau diminuarea vulnerabilităților care au cauzat incidentul.

8. Serviciul Management Integrat IT este responsabil cu documentarea anchetei privind incidentul.

9. Serviciul Management Integrat IT este responsabil de coordonarea activităților de comunicare cu terți pentru rezolvarea incidentului.

10. În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare Serviciul Management Integrat IT va recomanda sancțiuni disciplinare.

11. În cazul în care incidentul implică aplicarea legilor civile sau penale Serviciul Management Integrat IT va recomanda sesizarea organelor în drept ale statului şi va acționa ca ofițer de legătură cu acestea.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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/

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

3. http://www.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 monitorizare a Resurselor Informatice şi de Comunicaţii

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de monitorizare a Resurselor Informatice şi de Comunicaţii

Introducere

Monitorizarea RIC pentru asigurarea securităţii sistemului este o metodă utilizată pentru a confirma funcţionalitatea şi eficienţa măsurilor de securitate. Această activitate constă în următoarele (fără a se limita numai la aceste exemple):

- Detectarea automată a intruşilor prin intermediul sistemelor de înregistrare (logare).
- Jurnale *Firewall*
- Jurnale ale activităţii conturilor utilizator
- Jurnale ale scanărilor reţea
- Jurnale ale aplicaţiilor
- Jurnale ale solicitărilor de suport tehnic
- Jurnale ale erorilor din sisteme şi servere.

Scopul

Scopul Regulamentului de Monitorizare a RIC este stabilirea regulilor şi procedurilor pentru verificarea funcţionalităţii şi eficienţei măsurilor de securitate. De asemenea această activitate urmăreşte detectarea situaţiilor de evitare sau dezactivare a controalelor. Unul din beneficiile monitorizării securităţii este identificarea din timp a tentativelor de fraudă sau a infracţiunilor şi a vulnerabilităţilor sistemelor componente ale RIC. Alte beneficii includ: rezolvarea reclamaţiilor, monitorizarea serviciilor, estimarea performanţelor sistemelor în vederea întocmirii planurilor de modernizare, etc.

Audienta

Regulamentul de Monitorizare a RIC al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *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.
- *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.
- *Rețea locală (LAN):* O rețea de comunicații de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Rețeaua locală oferă comunicații între calculatoare și periferice la o viteză de transfer mare și cu puține erori

REGULAMENT de monitorizare a Resurselor Informatice și de Comunicații

1. Monitorizarea Resurselor Informatice și de Comunicații (RIC) se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări și înregistra:

   - Tipul traficului (ex. structura pe protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Tipul protocoalelor și a echipamentelor conectate la RIC, conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

2. Fișierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentele de securitate ale Universității. În această categorie intră următoarele (fără a se limita doar la acestea):

   - Jurnale ale sistemelor de detectare automată a intruşilor;

   - Jurnale *Firewall*;

   - Jurnale ale activității conturilor utilizator;

   - Jurnale ale scanărilor rețea;

   - Jurnale ale aplicațiilor;

   - Jurnale ale solicitărilor de suport tehnic;

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- Jurnale ale erorilor din sisteme şi servere.

3. Serviciul Management Integrat IT, sau personalul autorizat al Departamentelor / Centrelor sau Facultăților, va efectua, în mod regulat (cel puțin o dată la şase luni), verificări pentru detectarea:
   - Echipamentelor de rețea conectate neautorizat;
   - Parolelor utilizator care nu respectă regulamentele
   - Serviciilor de rețea neautorizate;
   - Serverelor de pagini de web neautorizate;
   - Echipamentelor ce utilizează resurse comune nesecurizate;
   - Utilizării de modem-uri neautorizate;
   - Licențelor pentru sistemele de operare şi programele instalate.
4. Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Serviciul Management Integrat IT în scopul efectuării de investigații.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal 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

pentru Detectarea Accesului Neautorizat

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT pentru Detectarea Accesului Neautorizat

Introducere

Detectarea tentativelor de acces neautorizat are un rol important în implementarea şi aplicarea unui regulament de securitate. Pe măsură ce complexitatea sistemelor informaționale şi de comunicații creşte, sistemele de securitate trebuie să evolueze. Odată cu creşterea numărului de vulnerabilități prin utilizarea sistemelor distribuite este necesar un mecanism de asigurare a securității la nivel de sistem precum şi la nivel de rețea. Sistemele de detectare a accesului neautorizat pot contribui la atingerea acestui scop.

Scopul

Detectarea tentativelor de acces neautorizat furnizează două funcții importante pentru protejarea resurselor informatice:

Feedback: informații referitoare la eficiența componentelor din sistemul de securitate. Dacă nu se detectează tentative sau chiar acces neautorizat în condițiile în care se foloseşte un sistem de detectare se consideră că mecanismele de apărare funcționează.

Trigger: un mecanism automat care determină când este necesară activarea anumitor măsuri specifice ca răspuns la un incident privind accesul neautorizat.

Audienta

Regulamentul privind Detectarea Tentativelor de Acces Neautorizat în sistemul RIC al Universității din Oradea, se aplică tuturor persoanelor responsabile de instalarea de noi RIC precum şi persoanelor care răspund de utilizarea RIC existente şi persoanelor însărcinate cu Securitatea RIC.

Definiții

- *Resurse Informatice şi de Comunicații* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi 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 şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- *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.
- *Incident de Securitate*: În termeni informatici, este definit ca un eveniment de încercare de pătrundere, o intrare neautorizată sau un atac asupra informației de pe un sistem automatizat din cadrul RIC. Definiția include examinarea sau navigarea neautorizată, întreruperea sau anularea serviciilor, alterarea sau distrugerea datelor, a mediilor de stocare sau a datelor de ieșire, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără știrea, indicațiile sau intenția utilizatorului.
- *Atac informațional*: O încercare de a trece peste măsurile și controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informațiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular și de eficacitatea contramăsurilor aplicate.
- *Protecție informațională*: Acțiuni întreprinse în vederea afectării informațiilor și sistemelor informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii.
- *Gazdă (Host):* Un sistem care oferă servicii pentru un anumit număr de utilizatori.
- *Server*: Un program care oferă servicii altor programe aflate pe același sistem de calcul sau pe alte sisteme conectate în rețea. Un sistem de calcul care rulează un program de tip server este adesea numit server, cu toate că pe același calculator mai pot rula și alte programe de tip client sau server.
- *Firewall*: Un mecanism de control al accesului care acționează ca o barieră între două sau mai multe segmente ale unei rețele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja rețelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

REGULAMENT pentru Detectarea Accesului Neautorizat

1. Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).

2. Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de *firewall*-uri și sistemele de control al accesului la rețea.

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

3. Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele *firewall* şi pe toate sistemele de control al accesului.

4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.

5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip *firewall* sau dispozitive de control al accesului.

6. Înregistrările de verificare pentru serverele şi host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal.

7. Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.

8. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

9. Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Serviciul Management Integrat IT.

10. Utilizatorii sunt obligați să raporteze Serviciului Management Integrat IT orice anomalii în performanța sistemelor utilizate sau orice semne ale unor posibile infracțiuni.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 crearea şi utilizarea copiilor de siguranță (backup)

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

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT privind crearea şi utilizarea copiilor de siguranţă (backup)

Introducere

Copiile de siguranţă (*backup*) sunt necesare pentru a permite recuperarea datelor şi aplicaţiilor în cazul unor evenimente cum ar fi: dezastre naturale, defecţiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcţionare a sistemului etc.

Scopul

Scopul Regulamentului de Back-up al Universităţii din Oradea este de a stabili regulile pentru crearea copiilor de siguranţă (backup) şi stocarea informaţiilor electronice ale Universităţii din Oradea.

Audienta

Regulamentul privind Crearea Copiilor de Siguranţă (*backup*) al Universităţii din Oradea se aplică tuturor persoanelor din cadrul Universităţii din Oradea care sunt responsabile cu instalarea şi întreţinerea de RIC, persoanelor însărcinate cu securitatea RIC şi deţinătorilor de informaţii.

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.
- *Copii de Siguranţă* (*backup*): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.
- *Stocarea Externă* (*Offsite*): Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de campus-ul universitar în care este puţin probabil să se producă efecte de acelaşi tip în cazul unui dezastru. Pe baza unei evaluări a informaţiei pentru care s-au realizat copii de siguranţă, mutarea mediilor de backup din clădire şi depozitarea lor într-o altă zonă securizată din campusul Universităţii din Oradea poate înlocui stocarea externă.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 27.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Furnizor:* Persoană fizică/juridică care oferă bunuri sau servicii Universității din Oradea în baza unui contract comercial sau de colaborare.

Servicii

SMIIT, administratorul RIC poate avea contracte pentru stocarea copiilor de siguranță (*backup*) în alte zone. Aceste servicii pot fi extinse, la cerere, către toate Departamentele / Centrele şi Facultățile din Universitatea din Oradea.

REGULAMENT privind crearea şi utilizarea copiilor de siguranță (backup)

1. Frecvența, dimensiunea şi conținutul copiilor de siguranță trebuie să fie în concordanță cu importanța informației şi cu riscul acceptat de proprietarul datelor.

2. Procedura de creare a copiilor de siguranță şi de recuperare pentru fiecare sistem din cadrul Resurselor Informatice şi de Comunicații trebuie să fie documentată şi periodic revizuită.

3. Furnizorul care oferă servicii de stocare a copiilor de siguranță în alte zone pentru Universitate trebuie să fie acreditat în acest scop de către o autoritate a statului.

4. Procedurile stabilite între Universitate şi furnizorii de stocare a copiilor de siguranță în altă zonă trebuie să fie revizuite cel puțin anual.

5. Verificarea copiilor de siguranță se va face după o procedură documentată şi revizuită periodic.

6. Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.

7. Accesul la mediile de *backup* ale Universității stocate la furnizori externi sau în interior se va face folosindu-se proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.

8. Benzile sau mediile utilizate pentru stocarea copiilor de siguranță trebuie să aibă un sistem de identificare care să conțină cel puțin următoarele date de identificare a informației stocate:

- numele sistemului;
- data creării copiei;
- tipul de copie (completă, incrementală etc.);
- clasificarea sensibilității (siguranței/securității);
- informații de contact.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE _____
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Securizare a Serverelor

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

APROBAT ÎN SEDINTA DE SENAT DIN
DATA DE 27.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de Securizare a Serverelor

Introducere

Serverele sunt acele sisteme care stochează şi distribuie informaţia către utilizatorii autorizaţi. În acest context trebuie asigurată integritatea, confidenţialitatea şi disponibilitatea datelor prin instalarea şi menţinerea acestora într-o manieră care să prevină accesul neautorizat, utilizarea neautorizată şi întreruperea unor servicii.

Scopul

Scopul Regulamentului de Securizare a Severelor din Universitatea din Oradea este de a prezenta cerinţele de instalare a unui nou server si de a menţine integritatea securităţii acestuia şi a aplicaţiilor.

Audienta

Regulamentul de Securizare a Severelor al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

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)

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Server:* Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

REGULAMENT de Securizare a Serverelor

1. Un server va fi conectat la rețeaua Universității din Oradea numai dacă se află într-o stare sigură, acreditată de către Serviciul Management Integrat IT.
2. Procedura de securizare a serverelor trebuie să includă, obligatoriu, următoarele:
   - Instalarea sistemului de operare dintr-o sursă aprobată;
   - Aplicarea *patch*-urilor furnizate de producător;
   - Înlăturarea programelor, a serviciilor sistem şi a driver-elor care nu sunt necesare;
   - Setarea/activarea parametrilor de securitate, a protecțiilor pentru fişiere şi activarea jurnalelor de monitorizare;
   - Dezactivarea sau schimbarea parolelor conturilor predefinite;
   - Securizarea accesului fizic la aceste echipamente.
1. Serviciul Management Integrat IT, în colaborare cu administratorii de sistem ai structurilor UO, va monitoriza, în mod obligatoriu, procesul de instalare a serverelor principale (*enterprise*) şi aplicarea regulată a *patch*-urilor de securitate. De asemenea, va monitoriza, prin sondaj, procesul de instalare şi aplicarea regulată a *patch*-urilor de securitate pentru serverele departamentale / centrelor sau a grupurile de lucru.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

7. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Utilizare a reţelei Internet şi Intranet

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Regulament de Utilizare a rețelei Internet şi Intranet

Introducere

În acord cu prevederile din prezentul Regulament, Resursele Informatice şi de Comunicații (RIC) sunt bunuri strategice ale Universității din Oradea care trebuie administrate ca resurse ale statului român. Acest regulament este stabilit pentru a atinge următoarele scopuri:

1. Să fie în conformitate cu statutele, regulamentele şi alte documente oficiale în vigoare pentru administrarea resurselor informatice,
2. Să stabilească practici prudente şi acceptabile privind utilizarea rețelei Internet,
3. Să instruiască utilizatorii care pot folosi rețeaua Internet în ceea ce priveşte responsabilitățile lor asociate unei astfel de utilizări.

Audienta

Regulamentul de Utilizare Internet şi Intranet se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității din Oradea care are capacitatea de acces Internet şi/sau Intranet.

Definiții

- *Resurse Informatice şi de Comunicații* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi 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 şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația.
- *Inginerul de sistem/Administratorul de rețea* îndeplineşte şi funcția 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 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.

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 27.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Internet*: Sistem global care interconectează calculatoare şi rețele de calculatoare. Acestea sunt deținute de mai multe organizații, agenții guvernamentale, societăți, instituții academice.
- *Intranet*: Rețea privată destinată comunicațiilor şi partajării informațiilor, care, ca şi rețeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizați din cadrul unei organizații (instituții). În mod obişnuit, rețeaua Intranet a unei organizații este protejată printr-un sistem de protecție (*firewall*).

Drept de proprietate

Fişierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia şi sub controlul Universității din Oradea, cad sub incidența reglementărilor legale privind proprietatea intelectuală.

Confidential

Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia şi sub controlul Universității din Oradea ~~nu~~ sunt confidențiale şi pot fi accesate de către personalul responsabil cu securitatea RIC, în condițiile prevăzute de lege. ~~Conținutul unui fişier electronic poate fi accesat de către personalul autorizat în conformitate cu prevederile şi normele de securitate ce se regăsesc în Regulamentul privind Accesul Administrativ.~~

Regulament de Utilizare a rețelei Internet şi Intranet

1. Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopuri academice şi de cercetare.
2. Toate programele utilizate pentru acces la rețeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Serviciul Management Integrat IT. Aceste programe trebuie să includă toate *patch*-urile de securitate puse la dispoziție de către producător.
3. Toate fişierele care provin din rețeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puțin o dată la 24 ore.
4. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor *proxy* şi/sau *firewall*.
5. Toate informațiile accesate în rețeaua Internet trebuie să se conformeze Regulamentului de Utilizare a RIC.
6. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
7. Conținutul tuturor site-urilor web ale Universității trebuie să se conformeze Regulamentelor de Utilizare a RIC.
8. Nu se vor publica pe site-urile web ale Universității materiale cu caracter ofensiv sau de hărțuire.
9. Nu se vor publica pe site-urile web ale Universității materiale publicitare comerciale sau personale.
10. Nu se vor publica pe sit-urile web ale Universității din Oradea date ale Universității din Oradea fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 14.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

11. Nu este permisă utilizarea RIC ale Universității în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea.
12. Cumpărăturile pe Internet care nu au legătură cu atribuțiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziție ale Universității.
13. Orice material confidențial al Universității transmis prin rețeaua Internet trebuie criptat.
14. Fișierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament / Centru sau Facultate.

Utilizare ocazionala

1. Utilizarea personală ocazională a RIC pentru acces la rețeaua Internet este permisă doar utilizatorilor care au aprobarea Universității din Oradea; acest drept nu se extinde membrilor familiei sau altor persoane.
2. Utilizarea ocazională nu trebuie să aibă ca rezultat costuri directe pentru Universitatea din Oradea.
3. Utilizarea ocazională nu trebuie să afecteze îndeplinirea sarcinilor de serviciu ale angajatului sau activitatea studenților.
4. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Universității din Oradea, sau punerea acesteia într-o situație delicată.
5. Stocarea fișierelor şi documentelor personale pe Resursele Informatice ale Universității din Oradea, trebuie să fie nominală.
6. Toate fișierele şi documentele – inclusiv cele personale – stocate sau transportate prin intermediul RIC sunt proprietatea Universității din Oradea, în condițiile legilor în vigoare. Acestea pot fi subiectul cererilor de deschidere a raporturilor, şi pot fi accesate în conformitate cu Regulamentul de Acces Administrativ.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

7. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI CERCETĂRII TINERETULUI SI SPORTULUI
UNIVERSITATEA DIN ORADEA
Adresa: Str. Universității nr.1, Oradea, România
Telefon: +40 259 432830 Fax: +40 259 432789
E-mail: rectorat@uoradea.ro Pagina web: www.uoradea.ro
CUI 4287939

REGULAMENT privind Configurarea Sistemelor Informatice pentru Acces la Rețeaua de Comunicații

Introducere

Rețeaua de comunicații a Universității 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 distribuție și nodurile principale. Este important ca aceasta să se dezvolte controlat și continuu în condiții de flexibilitate și evolutivitate. Este important ca dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate și diferențiate cât și cerințele privind securitatea întregului ansamblu.

Audienta

Regulamentul de Acces la Rețeaua de Comunicații a Universității din Oradea se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC

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

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

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

REGULAMENT privind Configurarea Sistemelor Informatice pentru Acces la Rețeaua de Comunicații

1. Infrastructura de comunicații, rețeaua de comunicații digitale a Universității este administrată de către Serviciul Management Integrat IT care este responsabilă cu întreținerea şi dezvoltarea acesteia.
2. Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare toate componentele acesteia sunt instalate de către Serviciul Management Integrat IT (SMIIT) sau de către un furnizor avizat explicit de către Serviciul Management Integrat IT.
3. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor Serviciului Management Integrat IT.
4. Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații se face numai cu aprobarea Serviciului de Management Integrat IT.
5. Infrastructura de comunicații de date a Universității suportă un set definit de protocoale de rețea. Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către Serviciul Management Integrat IT.
6. Adresele de rețea sunt alocate dinamic sau static numai de către Serviciul Management Integrat IT.
7. Numerele de telefon sunt alocate numai de către SMIIT.
8. Toate conectările în rețeaua de comunicații a Universității sunt responsabilitatea Serviciului Management Integrat IT, conectarea se va face numai în baza unei cereri standard aprobată de către Departament / Centru / Facultate sau structura UO. Formularele vor fi puse la dispoziție prin intermediul site-ului web al Serviciului Management Integrat IT.
9. Toate conectările dintre rețeaua de comunicații a Universității şi alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a Serviciului Management Integrat IT.
10. Utilizarea sistemelor de protecție (*firewall*) din Departamente / Centre şi Facultăți nu este permisă fără autorizație scrisă din partea Serviciului Management Integrat IT. Această restricție se aplică şi în cazul în care se folosesc adrese private de rețea.
11. Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile rețelei (este interzisă instalarea unui, fax, modem, router, switch, hub sau punct de acces la rețeaua Universității) fără aprobare din partea Serviciului Management Integrat IT.
12. Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau programe care furnizează servicii de rețea fără aprobarea Serviciului Management Integrat IT.
13. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale rețelei.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal 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

privind parolele de acces

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT privind parolele de acces

Introducere

Autentificarea este necesară pentru a controla accesul utilizatorilor la Resursele Informatice şi de Comunicaţii (RIC). Controlul accesului este necesar deoarece accesul neautorizat poate duce la prejudicii cauzate de afectarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor. Acestea pot avea ca efecte pierderi materiale şi morale pentru Universitatea din Oradea. Autentificarea utilizatorilor se poate realiza folosind diverse metode: conturi şi parole de acces, dispozitive de identificare, caracteristici biologice.

Scopul

Regulamentul pentru Parole de Acces al Universităţii din Oradea stabileşte reguli şi proceduri obligatorii pentru crearea şi modificarea parolelor de acces la RIC.

Audienta

Regulamentul pentru Parole de Acces al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

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* □ndeplineşte 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 □nfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- ***Utilizator*: O persoană, o aplicație automatizată sau process utilizator** autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Parole complexe:* O parolă complexă este un şir de caractere (secvență de caractere, numere şi caractere speciale) care nu poate fi asociată cu informația publică despre contul utilizator, nu este copiată dintr-un dicționar etc.

REGULAMENT privind parolele de acces

Criterii pentru Alegerea unei parole:

1. Orice parolă ar trebui să fie complexă şi să aibă o lungime minimă de 8 caractere.

   O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^* ...).
2. Nu este deloc recomandată folosirea simplă a datelor personale (ex: data naşterii, nume, prenume etc.) ca parole
3. Parolele trebuie să respecte următoarele condiții:
   - Nu trebuie să coincidă sau să fie asemănătoare cu numele dvs. de utilizator (login-ul);
   - Nu trebuie să coincidă sau să fie asemănătoare cu numărul dvs. de angajat;
   - Nu trebuie să coincidă sau să fie asemănătoare cu numele dvs.;
   - Nu trebuie să coincidă sau să fie asemănătoare cu numele membrilor familiei;
   - Nu trebuie să coincidă sau să fie asemănătoare cu o eventuală poreclă (*nickname*);
   - Nu trebuie să coincidă cu codul numeric personal;
   - Nu trebuie să coincidă cu data naşterii;
   - Nu trebuie să coincidă cu numărul de înmatriculare al maşinii;
   - Nu trebuie să coincidă cu adresa;
   - Nu trebuie să fie numărul dvs. de telefon;
   - Nu trebuie să coincidă cu numele oraşului;
   - Nu trebuie să coincidă cu numele departamentului etc.;
   - Nu trebuie să coincidă cu nume de străzi;
   - Nu trebuie să coincidă cu mărci sau modele de maşini;
   - Nu trebuie să coincidă cu argouri;
   - Nu trebuie să coincidă cu obscenități;
   - Nu trebuie să fie termeni tehnici;
   - Nu trebuie să coincidă cu numele, mascota sau sloganul unei şcoli;
   - Nu trebuie să coincidă cu informații despre proprietarul contului care sunt cunoscute sau uşor de ghicit (mâncarea, culoarea preferată, sportul preferat etc.);
   - Nu trebuie să coincidă cu un acronim popular;
   - Nu trebuie să fie cuvinte din dicționar;
   - Nu trebuie să fie opusul tuturor celor de mai sus.
   - Parolele nu trebuie să fie reutilizate pentru o perioadă de un an.
   - Parolele nu trebuiesc divulgate în nici o situație.
   - Parolele trebuiesc tratate ca informație confidențială.

Reguli pentru utilizarea parolelor:

1. Toate parolele trebuie să îndeplinească următoarele condiții:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

a. Să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile;
b. Să aibă o lungime minimă de 8 caractere;
c. Să fie parole complexe;
d. Reutilizarea parolelor este interzisă;
e. Parolele stocate trebuie criptate;
f. Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice.

2. Nu vă notați parolele pe hârtii.
3. Nu folosiți aceeași parolă pentru mai multe conturi.
4. Dacă aveți multe parole le puteți scrie într-un fișier, însă criptați acel fișier și asigurați-vă că nu-l veți pierde. Evitați denumirea acelui fișier cu una explicită (parolelemele.rar).
5. Evitați să pastrați parole în agende electronice, telefoane mobile – pot fi furate.
6. Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepții pentru anumite aplicații (precum backup automat) cu aprobarea Inginerului de sistem/Administratorului de rețea. Pentru ca o excepție să fie aprobată, trebuie să existe o procedură pentru schimbarea parolelor.
7. Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile.
8. Aveți grijă la facilitatea browser-elor de reținere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucrați e folosit de mai multe persoane.
9. Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice.
10. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
11. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
12. Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.
13. Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
    - utilizatorul se va legitima;
    - administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
    - utilizatorul va introduce o nouă parolă.
14. Dispozitivele de securitate (ex. card *Smart*) trebuiesc returnate după terminarea relațiilor cu Universitatea din Oradea.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 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.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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.	Hotărîrea SUO nr.
Data:	Data:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de administrare a conturilor de email

Introducere

Conturile utilizator sunt mijloacele utilizate pentru a permite accesul la RIC ale Universității din Oradea. Astfel, crearea, modificarea, controlul şi monitorizarea conturilor utilizator sunt operațiuni foarte importante în cadrul general al asigurării securității 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 Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor care au acces autorizat la sistemul de RIC din cadrul Universității din Oradea

Definiții

- *Resurse Informatice şi de Comunicații* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi 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 şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația.
- *Inginerul de sistem/Administratorul de rețea* îndeplineşte şi funcția 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 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 şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.

---

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

[2] Până la □nființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
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.

APROBAT ÎN SEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 sistemul de mesagerie electronica

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

APROBAT ÎN SEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT privind sistemul de mesagerie electronica

Introducere

Acest regulament este stabilit astfel încât:

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

Scopul

Scopul Regulamentului privind Sistemul de Mesagerie Electronică al Universităţii din Oradea, este de a stabili regulile pentru utilizarea serviciului de poştă electronică din cadrul Universităţii din Oradea, privind trimiterea, primirea sau stocarea mesajelor asociate poştei electronice.

Audienta

Regulamentul privind Sistemul de Mesagerie Electronică al Universităţii din Oradea, se aplică nediscriminatoriu tuturor persoanelor care au permisiuni de acces la orice resursă informatică din cadrul Universităţii care are capacitatea de a trimite, primi sau stoca mesaje asociate poştei electronice.

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.
- *Sistem de Mesagerie Electronică*: orice program care permite ca mesajele în format electronic să fie transmise de la un sistem de calcul la altul.
- *Mesagerie Electronică*: orice mesaj, imagine, formular, ataşament, date sau orice alt mijloc de comunicaţie, trimise, primite sau stocate într-un sistem de mesagerie electronică.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

REGULI privind sistemul de mesagerie electronica

I. Activităţi strict interzise

- Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
- Folosirea sistemului de mesagerie electronică în scopuri personale;
- Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

II. Activităţi interzise deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:

- Trimiterea sau retrimiterea email-urilor în lanţ;
- Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
- Trimiterea mesajelor de dimensiuni foarte mari;
- Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.
- Ignorarea cererii administratorului reţelei de a elibera spaţiile de pe server pe care le ocupă. Conform Regulilor de administrare a conturilor de email, toţi utilizatorii (cu excepţia persoanelor care au funcţii de conducere şi a celor din secretariate) se obligă să menţină în directoarele proprii de pe serverul de mail numai mesajele din cel mult ultimele 14 zile.

III. Alte menţiuni

- Toţi utilizatorii sistemului RIC, fără excepţie, vor folosi adrese e-mail din domeniul uoradea.ro (toate adresele e-mail vor avea sufixul uoradea.ro).
- Toate informaţiile şi datele confidenţiale ale Universităţii, transmise către alte reţele externe, trebuie să fie criptate.
- Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea resurselor informatice şi de comunicaţii ale Universităţii pot fi oricând înregistrate şi analizate, în condiţiile respectării prevederilor legale privind confidenţialitatea informaţiei.
- Utilizatorii serviciilor de mesagerie electronică nu sunt abilitaţi să reprezinte, să îşi spună opinia sau să dea declaraţii în numele Universităţii, cu excepţia situaţiilor în care sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă Universitatea. Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu reprezintă un punct de vedere oficial al Universităţii din Oradea"
- Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc Universitatea din Oradea, folosind conturi utilizator care nu sunt proprietatea Universităţii din Oradea. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: gmail, Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi Furnizorii de Servicii Internet.

APROBAT ÎN SEDINTA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc Universitatea, folosind dispozitive de comunicații mobile care nu sunt autorizate de Universitate. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: telefoane mobile, asistenți digitali personali, pagere ce permit trimiterea/primirea de informații.
- Rețeaua UONet se declară a fi un mediu de lucru şi comunicare academic, deschis şi civilizat. Utilizatorii sunt invitati să se trateze reciproc în mod politicos şi cordial. Spiritul Internet presupune dialoguri într-un stil caracterizat prin decență, amabilitate şi bunăvoință. Partenerii nostrii din Internet se aşteaptă să găsească în UO şi un mediu academic atunci când solicită informații despre noi, motiv pentru care, utilizatorii vor lua măsuri pentru a se autoidentifica corect atât pe serverul din uoradea, cât şi în corespondența electronică pe care o trimit.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

APROBAT ÎN SEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 detectarea viruşilor

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT privind detectarea virusilor

Introducere

Numărul incidentelor de securitate şi costurile ce rezultă din întreruperea şi restabilirea serviciilor RIC sunt în continuă creştere. Câteva dintre acţiunile care pot fi luate pentru reducerea riscurilor şi scăderea costurilor incidentelor de securitate sunt: implementarea unor reguli severe de securitate, blocarea accesului inutil la RIC, detectarea în timp util şi minimizarea efectelor cauzate de incidente de securitate.

Scopul

Scopul Regulamentului de Detectare a Virusilor din RIC este de a descrie măsuri ce trebuie luate pentru prevenirea, detectarea şi îndepărtarea programelor de tip virus, vierme sau altele asemănătoare.

Audienta

Regulamentul de Detectare a Virusilor a Resurselor Informatice şi de Comunicaţii al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

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.

---

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Virus*: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte deranjante sau distructive. Un fişier virus se execută în momentul în care este accesat un fişier infectat.
- *Vierme*: Un program care se auto-copiază într-o altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care se multiplică într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii din cauză că folosesc resursele RIC pentru a se multiplica, cauzând încărcare suplimentară a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere sau sectoare pentru a se multiplica.
- *Cal Troian*: De obicei un program de tip virus sau vierme care este ascuns sub aparenţa unui program atractiv sau inofensiv. Victimele pot primi un astfel de virus prin email sau prin transfer prin reţea sau de pe un mediu de stocare extern.

REGULAMENT privind detectarea virusilor

1. Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus.

2. Programele antivirus nu trebuie dezactivate.

3. Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

4. Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

5. Orice server de fişiere conectat la reţeaua instituţiei trebuie să utilizeze un program antivirus în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

6. Orice server sau *gateway* pentru e-mail trebuie să folosească un program antivirus pentru e-mail şi trebuie să respecte regulile de instalare şi de utilizare a acestui program.

7. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Serviciului Management Integrat IT.

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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Referințe

1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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

PROCEDURA

pentru Alocarea unei Adrese de Email

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 12.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

PROCEDURĂ pentru Alocarea unei Adrese de Email

Scop:

Procedura stabileste principiile ce stau la baza stabilirii adreselor de email si pasii ce trebuiesc parcursi in vederea obtinerii unei adrese de email.

Audienta:

Se adresează cadrelor didactice, cercetătorilor, doctoranzilor, personalului de administrație din Universitatea din Oradea care doresc deschiderea unui cont de email pe domeniul uoradea.ro

Procedura

1. Toate cadrele didactice, toți doctoranzii, cercetătorii, precum şi toți angajații care aparțin personalului administrativ, auxiliar didactic sau nedidactic au dreptul de a deține o adresă de email pe serverul Universității.

2. Se recomandă ca adresa de email să fie de forma:

nume@uoradea.ro sau **prenume.nume@uoradea.ro** sau **inume@uoradea.ro** (unde i reprezintă inițiala prenumelui)

3. Cererile de obținere a unui cont de email pe serverul Universității se downloadează de pe site-ul universitatii şi se depun la Serviciul Management Integrat IT – anexa 1.

4. Pentru verificarea căsuței poştale este pusă la dispoziție o interfață web la adresa http://mail.uoradea.ro

Se poate accesa de pe orice calculator conectat la Internet, prin intermediul unui browser (Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari etc.)

De asemenea, pe calculatorul fiecărui utilizator se va configura un client local de email (exemple: Mozilla Thunderbird, Outlook express). Motivul principal este acela că, pentru a se asigura o funcționare optimă a serviciului de email, utilizatorilor nu le este permis să păstreze în directoarele proprii de pe server mesaje mai vechi de 14 zile.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Anexa 1

Formular pentru alocarea de adresa de e-mail

1. Date de identificare:

Nume

Prenume

Fucția

Facultatea

Departament

Telefon birou

☐ Cadru didactic ☐ Angajat ☐ Doctorand ☐ Altele

2. Date referitoare la adresa de e-mail:

Nume utilizator:

Propus:

Alocat:

Parola (acordată de administratorul de sitem):

Subsemnatul(a), **declar ca voi respecta** "Politica de securitate a Universității din Oradea" şi voi ține cont de **recomandările făcute**.

Data:

Semnătura

Oradea

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Rețeaua de Comunicații

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de Acces la Rețeaua de Comunicații

Introducere

Rețeaua de comunicații a Universității 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 distribuție și nodurile principale. Este important ca aceasta să se dezvolte controlat și continuu în condiții de flexibilitate și evolutivitate. Este important ca dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate și diferențiate cât și cerințele privind securitatea întregului ansamblu.

Scopul

Scopul Regulamentului de Acces la Rețeaua de Comunicații a Universității din Oradea constă în stabilirea regulilor de acces și utilizare a acesteia. Aceste reguli sunt necesare pentru păstrarea integrității, disponibilității și confidențialității informației din cadrul RIC ale Universității din Oradea.

Audienta

Regulamentul de Acces la Rețeaua de Comunicații a Universității din Oradea se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC

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.

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității 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 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 la Rețeaua de Comunicații

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

2. Departamentele / Centrele şi Facultățile trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Universității. 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 Universității nu se pot conecta la altă rețea.

6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în nici un fel, pe nici o cale. Nu este permisă instalarea de conexiuni de rețea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăților / Centrelor şi a Departamentelor de către Serviciul Management Integrat IT.

8. Sistemele computerizate din afara Universității care necesită conectare la rețea trebuie să se conformeze cu standardele rețelei interne ale Universității.

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 Universității nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectați la rețeaua Universității.

10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, 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 rețelei Universității cu alte rețele sunt realizate exclusiv de către Serviciul de Management Integrat IT.

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

[3] Trebuie reglementat acest aspect

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 11.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 monitorizare a Resurselor Informatice şi de Comunicaţii

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT de monitorizare a Resurselor Informatice şi de Comunicaţii

Introducere

Monitorizarea RIC pentru asigurarea securităţii sistemului este o metodă utilizată pentru a confirma funcţionalitatea şi eficienţa măsurilor de securitate. Această activitate constă în următoarele (fără a se limita numai la aceste exemple):

- Detectarea automată a intruşilor prin intermediul sistemelor de înregistrare (logare).
- Jurnale *Firewall*
- Jurnale ale activităţii conturilor utilizator
- Jurnale ale scanărilor reţea
- Jurnale ale aplicaţiilor
- Jurnale ale solicitărilor de suport tehnic
- Jurnale ale erorilor din sisteme şi servere.

Scopul

Scopul Regulamentului de Monitorizare a RIC este stabilirea regulilor şi procedurilor pentru verificarea funcţionalităţii şi eficienţei măsurilor de securitate. De asemenea această activitate urmăreşte detectarea situaţiilor de evitare sau dezactivare a controalelor. Unul din beneficiile monitorizării securităţii este identificarea din timp a tentativelor de fraudă sau a infracţiunilor şi a vulnerabilităţilor sistemelor componente ale RIC. Alte beneficii includ: rezolvarea reclamaţiilor, monitorizarea serviciilor, estimarea performanţelor sistemelor în vederea întocmirii planurilor de modernizare, etc.

Audienta

Regulamentul de Monitorizare a RIC al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *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.
- *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.
- *Rețea locală (LAN):* O rețea de comunicații de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Rețeaua locală oferă comunicații între calculatoare și periferice la o viteză de transfer mare și cu puține erori

REGULAMENT de monitorizare a Resurselor Informatice și de Comunicații

1. Monitorizarea Resurselor Informatice și de Comunicații (RIC) se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări și înregistra:

   - Tipul traficului (ex. structura pe protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Tipul protocoalelor și a echipamentelor conectate la RIC, conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

2. Fișierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentele de securitate ale Universității. În această categorie intră următoarele (fără a se limita doar la acestea):

   - Jurnale ale sistemelor de detectare automată a intruşilor;

   - Jurnale *Firewall*;

   - Jurnale ale activității conturilor utilizator;

   - Jurnale ale scanărilor rețea;

   - Jurnale ale aplicațiilor;

   - Jurnale ale solicitărilor de suport tehnic;

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la înființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- Jurnale ale erorilor din sisteme şi servere.

3. Serviciul Management Integrat IT, sau personalul autorizat al Departamentelor / Centrelor sau Facultăților, va efectua, în mod regulat (cel puțin o dată la şase luni), verificări pentru detectarea:
    - Echipamentelor de rețea conectate neautorizat;
    - Parolelor utilizator care nu respectă regulamentele
    - Serviciilor de rețea neautorizate;
    - Serverelor de pagini de web neautorizate;
    - Echipamentelor ce utilizează resurse comune nesecurizate;
    - Utilizării de modem-uri neautorizate;
    - Licențelor pentru sistemele de operare şi programele instalate.
4. Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Serviciul Management Integrat IT în scopul efectuării de investigații.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 crearea şi utilizarea copiilor de siguranţă (backup)

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 11.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

REGULAMENT privind crearea şi utilizarea copiilor de siguranţă (backup)

Introducere

Copiile de siguranţă (*backup*) sunt necesare pentru a permite recuperarea datelor şi aplicaţiilor în cazul unor evenimente cum ar fi: dezastre naturale, defecţiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcţionare a sistemului etc.

Scopul

Scopul Regulamentului de Back-up al Universităţii din Oradea este de a stabili regulile pentru crearea copiilor de siguranţă (backup) şi stocarea informaţiilor electronice ale Universităţii din Oradea.

Audienta

Regulamentul privind Crearea Copiilor de Siguranţă (*backup*) al Universităţii din Oradea se aplică tuturor persoanelor din cadrul Universităţii din Oradea care sunt responsabile cu instalarea şi întreţinerea de RIC, persoanelor însărcinate cu securitatea RIC şi deţinătorilor de informaţii.

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 Assistanţ* - 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.
- *Copii de Siguranţă* (*backup*): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.
- *Stocarea Externă* (*Offsite*): Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de campus-ul universitar în care este puţin probabil să se producă efecte de acelaşi tip în cazul unui dezastru. Pe baza unei evaluări a informaţiei pentru care s-au realizat copii de siguranţă, mutarea mediilor de backup din clădire şi depozitarea lor într-o altă zonă securizată din campusul Universităţii din Oradea poate înlocui stocarea externă.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- *Furnizor:* Persoană fizică/juridică care oferă bunuri sau servicii Universității din Oradea în baza unui contract comercial sau de colaborare.

Servicii

SMIIT, administratorul RIC poate avea contracte pentru stocarea copiilor de siguranță (*backup*) în alte zone. Aceste servicii pot fi extinse, la cerere, către toate Departamentele / Centrele și Facultățile din Universitatea din Oradea.

REGULAMENT privind crearea și utilizarea copiilor de siguranță (backup)

1. Frecvența, dimensiunea și conținutul copiilor de siguranță trebuie să fie în concordanță cu importanța informației și cu riscul acceptat de proprietarul datelor.

2. Procedura de creare a copiilor de siguranță și de recuperare pentru fiecare sistem din cadrul Resurselor Informatice și de Comunicații trebuie să fie documentată și periodic revizuită.

3. Furnizorul care oferă servicii de stocare a copiilor de siguranță în alte zone pentru Universitate trebuie să fie acreditat în acest scop de către o autoritate a statului.

4. Procedurile stabilite între Universitate și furnizorii de stocare a copiilor de siguranță în altă zonă trebuie să fie revizuite cel puțin anual.

5. Verificarea copiilor de siguranță se va face după o procedură documentată și revizuită periodic.

6. Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.

7. Accesul la mediile de *backup* ale Universității stocate la furnizori externi sau în interior se va face folosindu-se proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.

8. Benzile sau mediile utilizate pentru stocarea copiilor de siguranță trebuie să aibă un sistem de identificare care să conțină cel puțin următoarele date de identificare a informației stocate:

- numele sistemului;
- data creării copiei;
- tipul de copie (completă, incrementală etc.);
- clasificarea sensibilității (siguranței/securității);
- informații de contact.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN SEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Utilizare a rețelei Internet şi Intranet

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

APROBAT ÎN ŞEDINTA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Regulament de Utilizare a rețelei Internet şi Intranet

Introducere

În acord cu prevederile din prezentul Regulament, Resursele Informatice şi de Comunicații (RIC) sunt bunuri strategice ale Universității din Oradea care trebuie administrate ca resurse ale statului român. Acest regulament este stabilit pentru a atinge următoarele scopuri:

1. Să fie în conformitate cu statutele, regulamentele şi alte documente oficiale în vigoare pentru administrarea resurselor informatice,
2. Să stabilească practici prudente şi acceptabile privind utilizarea rețelei Internet,
3. Să instruiască utilizatorii care pot folosi rețeaua Internet în ceea ce priveşte responsabilitățile lor asociate unei astfel de utilizări.

Audienta

Regulamentul de Utilizare Internet şi Intranet se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicații a Universității din Oradea care are capacitatea de acces Internet şi/sau Intranet.

Definiții

- *Resurse Informatice şi de Comunicații* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unități de stocare, şi 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 şi medical conectat la rețea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele şi datele care sunt proiectate, construite, puse în funcțiune (operaționale) şi menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informația.
- *Inginerul de sistem/Administratorul de rețea* □ndeplineşte şi funcția 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 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.

---

[1] Responsabil la nivelul instituției cu administrarea RIC ale Universității din Oradea
[2] Până la □nființarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- *Utilizator*: O persoană, o aplicație automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicații.
- *Internet*: Sistem global care interconectează calculatoare şi rețele de calculatoare. Acestea sunt deținute de mai multe organizații, agenții guvernamentale, societăți, instituții academice.
- *Intranet*: Rețea privată destinată comunicațiilor şi partajării informațiilor, care, ca şi rețeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizați din cadrul unei organizații (instituții). În mod obişnuit, rețeaua Intranet a unei organizații este protejată printr-un sistem de protecție (*firewall*).

Drept de proprietate

Fişierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia şi sub controlul Universității din Oradea, cad sub incidența reglementărilor legale privind proprietatea intelectuală.

Confidentialitate

Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia şi sub controlul Universității din Oradea ~~nu~~ sunt confidențiale şi pot fi accesate ~~oricând~~ de către angajații autorizați din cadrul Serviciului Management Integrat IT, Departamente / Departamente şi Facultăți în condițiile prevăzute de lege.

Regulament de Utilizare a rețelei Internet şi Intranet

1. Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopuri academice şi de cercetare.
2. Toate programele utilizate pentru acces la rețeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Serviciul Management Integrat IT. Aceste programe trebuie să includă toate *patch*-urile de securitate puse la dispoziție de către producător.
3. Toate fişierele care provin din rețeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puțin o dată la 24 ore.
4. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor *proxy* şi/sau *firewall*.
5. Toate informațiile accesate în rețeaua Internet trebuie să se conformeze Regulamentului de Utilizare a RIC.
6. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
7. Conținutul tuturor site-urilor web ale Universității trebuie să se conformeze Regulamentelor de Utilizare a RIC.
8. Nu se vor publica pe site-urile web ale Universității materiale cu caracter ofensiv sau de hărțuire.
9. Nu se vor publica pe site-urile web ale Universității materiale publicitare comerciale sau personale.
10. Nu se vor publica pe sit-urile web ale Universității din Oradea date ale Universității din Oradea fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

11. Nu este permisă utilizarea RIC ale Universității în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea.
12. Cumpărăturile pe Internet care nu au legătură cu atribuțiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziție ale Universității.
13. Orice material confidențial al Universității transmis prin rețeaua Internet trebuie criptat.
14. Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament / Centru sau Facultate.

Utilizare ocazionala

1. Utilizarea personală ocazională a RIC pentru acces la rețeaua Internet este permisă doar utilizatorilor care au aprobarea Universității din Oradea; acest drept nu se extinde membrilor familiei sau altor persoane.
2. Utilizarea ocazională nu trebuie să aibă ca rezultat costuri directe pentru Universitatea din Oradea.
3. Utilizarea ocazională nu trebuie să afecteze îndeplinirea sarcinilor de serviciu ale angajatului sau activitatea studenților.
4. Nu este permisă trimiterea sau recepționarea documentelor sau fişierelor care pot cauza acțiuni legale împotriva Universității din Oradea, sau punerea acesteia într-o situație delicată.
5. Stocarea fişierelor şi documentelor personale pe Resursele Informatice ale Universității din Oradea, trebuie să fie nominală.
6. Toate fişierele şi documentele – inclusiv cele personale – stocate sau transportate prin intermediul RIC sunt proprietatea Universității din Oradea, în condițiile legilor în vigoare. Acestea pot fi subiectul cererilor de deschidere a raporturilor, şi pot fi accesate în conformitate cu Regulamentul de Acces Administrativ.

Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi 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.dict.uvt.ro/regulamente/
4. 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:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

7. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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 şi libera circulație a acestor date.
16. 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 şi libera circulație a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Ghid de norme etice privind utilizarea Office 365 - Platforma SharePoint

1. Aspecte generale

Tehnologiile educaţionale bazate pe Office 365, vor constitui o componenta principală în pregatirea studentilor de la Universitatea din Oradea.

Serviciul Management Integrat IT din Universitatea din Oradea administrează accesul la această tehnologie , disponibilă la adresa web: https://uoradea.sharepoint.com

Capacitatea hardware şi structura software ale aceastei Platforme permit accesul simultan a tuturor utilizatorilor din Universitatea din Oradea (abreviat UO) (student, cadre didactice şi personal TESA).

Orice student de la UO poate beneficia de avantajele oferite de platforma Office 365 on-line independent şi indiferent de pozitia sa geografica.

In vederea realizarii dezideratelor de colaborare prin partajare şi comunicare în vederea optimizării procesului de dinstruire în conditii optime, este necesar sa fie respectate normele de etica a utilizării şi exploatarii Office 365 în cadrul Universităţii din Oradea.

Prezentul ghid de norme etice are drept obiectiv precizarea responsabilităţilor asumate de furnizorii, beneficiarii şi utilizatorii Platformei Office 365.

Printre valorile care stau la baza creării şi utilizării platformei se pot enumera:

1. promovarea valorilor academice, respectarea standardelor de formare şi educare în concordanta cu evoluţia pe plan mondial a educaţiei şi învatamântului, dar şi a societăţii în ansamblul său, respectarea legii, obiectivitatea, calitatea, transparenţa, formarea profesională continuă, confidenţialitatea, asigurarea drepturilor de autor, colaborarea şi non-discriminarea.
2. Responsabilitatea morală a utilizatorului şi a Administratorului Office 365.
3. Responsabilitatea morală a utilizatorului (cadru didactic, personal administrativ şi de secretariat şi student):

2. Condiţii pentru a fi membru

Serviciile sunt destinate studenţilor, personalului didactic şi personalului administrativ al Universităţii din Oradea.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Utilizatorii serviciului vor respecta acest **Ghid de norme etice privind utilizarea Office 365** şi vor fi responsabili pentru toate activităţile şi pentru tot conţinutul pe care publică/încărcă.

În afara respectării acestor norme de conduită, trebuie să se repecte toate legile locale sau naţionale aplicabile, precum și toate procedurile interne ale UO

3. Utilizări interzise

Conform normelor de conduită Microsoft Office365, se precizează că nu se va încărca, publica, transmite, transfera, distribui sau facilita distribuţia niciunui tip de conţinut (inclusiv text, imagini, sunet, video, date, informaţii sau software) şi nu se va utiliza serviciul în nicio manieră care:

- reprezintă nuditate de orice fel, inclusiv nuditate umană parţială sau totală sau nuditate în forme non-umane, cum ar fi în desene animate, artă fantastică sau manga.
- incită, promovează sau exprimă pornografie, obscenitate, vulgaritate, blasfemie, ură, bigotism, rasism sau violenţă gratuită.
- denaturează sursa oricărui material pe care îl publicaţi sau încărcaţi, inclusiv asumarea identităţii unei alte persoane sau entităţi.
- oferă sau creează linkuri la site-uri externe care încalcă aceste norme de conduită.
- include conţinut protejat prin legile drepturilor intelectuale, drepturile la intimitate sau la imagine publică sau prin orice altă normă legală, cu excepţia situaţiei în care deţineţi sau controlaţi drepturile respective sau aţi primit toate acordurile necesare.
- are ca scop lezarea sau exploatarea minorilor în orice mod.
- este creată pentru a solicita sau colecta informaţii ce pot identifica persoane minore (orice persoană sub 18 ani), inclusiv, dar fără a se limita la: nume, adresă de poştă electronică, adresă de domiciliu, număr de telefon sau numele şcolii.
- încalcă intimitatea oricărei persoane prin încercarea de a colecta, stoca sau publica informaţii private sau care identifică persoana, cum ar fi parole, informaţii despre cont, numere ale cărţilor de credit, adrese sau alte informaţii de contact, fără ştiinţa persoanei în cauză şi fără consimţământul ei voluntar.
- este ilegală sau încalcă legile locale şi naţionale aplicabile, inclusiv, dar fără a se limita la pornografie infantilă, bestialitate, incest, droguri ilegale, piraterie software şi hărţuire.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- ameninţă, hărţuieşte, calomniază, înşeală, degradează, victimizează sau intimidează o persoană sau un grup de persoane, indiferent de motiv, inclusiv pe motive de vârstă, sex, invaliditate, etnie, orientare sexuală, rasă sau religie, sau incită sau încurajează pe oricine altcineva la asemenea acţiuni.

- deteriorează sau întrerupe funcţionarea computerului unui alt utilizator sau încearcă să deterioreze sau să întrerupă funcţionarea computerului unui alt utilizator sau permite altor persoane să acceseze în mod ilegal software sau să treacă de măsurile de securitate de pe site-urile Web sau de pe servere, inclusiv dar fără a se limita la spam.

- încearcă să asume identitatea unui angajat, agent, manager, gazdă, administrator, moderator sau a altui utilizator Microsoft sau a altei persoane, prin orice mijloace.

- promovează sau facilitează în altă manieră cumpărarea sau vânzarea muniţiei sau a armelor de foc.

- conţine sau se poate considera „poştă electronică nedorită", „spam", „mesaje în lanţ", „scheme piramidale" sau „marketing afiliat" sau reclame comerciale nesolicitate.

- nu caracterizează în mod corect conţinutul pe care îl publicaţi sau încărcaţi sau conţine acelaşi conţinut sau conţinut similar cu cel pe care l-aţi publicat deja.

- încearcă să manipuleze serviciile, inclusiv sistemele de evaluare şi de reputaţie din servicii prin încălcarea prevederilor acestor norme de conduită, în colaborare cu alte persoane sau prin utilizarea mai multor profiluri.

- oferă efectuarea transferului internaţional al unor sume de bani mai mari decât preţul cerut pentru un articol, cu intenţia de a solicita restituirea oricărei părţi a plăţii.

- conţine reclame pentru scheme de îmbogăţire, carduri de reduceri, consultanţă privind creditele, sondaje şi concursuri online.

4. Drepturi şi responsabilităţi

Prezentul ghid de norme etice, privind utilizarea platformei Office 365 asigură respectarea regulamentelor de ordine interioara şi a Codului de etică al Universităţii din Oradea, contribuind la promovarea şi consolidarea rolului acestora.

Utilizatorii nu au dreptul să:

- Utilizeze serviciul online într-un mod care este interzis de orice lege, regulament, ordin sau decret guvernamental în orice jurisdicţie relevantă, sau care încalcă drepturile legale ale altor persoane;

APROBAT ÎN ŞEDINŢA DE SENAT DIN DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- utilizeze serviciul online într-un mod care ar putea pune în pericol sau afecta utilizarea acestuia de catre o altă persoană;
- utilizeze serviciul online pentru a încerca să obțineți acces neautorizat la orice serviciu, date, conturi sau rețele prin orice mijloace;
- falsifice informațiile de protocol sau de antet de e-mail (de exemplu, "*spoofing*");
- utilizeze serviciul online pentru a trimite "*spam*" (adică, mesaje nesolicitate sau mesaje comerciale), sau sa facă disponibile orice alte servicii destinate violării acestor termeni (de exemplu, atacurile de ti refuzul serviciului, etc);
- elimine, să modifice sau să încalce orice reglementare, notificare legală sau link care este încorporat în serviciul online

Compania Microsoft şi UO nu sunt răspunzătoare pentru conţinutul niciunei publicări, liste şi a niciunui mesaj create de utilizator. Decizia de a vizualiza conţinut sau de a lua legătura cu alte persoane, aparţine utilizatorilor care sunt sfătuiţi să procedeze raţional.

Utilizatorii sunt răspunzători pentru protejarea computerului propriu împotriva interferenţelor, a programelor spion sau a viruşilor care pot apărea în elementele descărcate de la serviciu. Se recomandă utilizarea unui program anti-virus pe computer care să fie menţinut la zi.

Microsoft şi UO îşi rezervă dreptul de a amenda sau a modifica normele de conduită sau orice serviciu în orice moment, fără notificare prealabilă. Se recomandă revederea periodică a acestor instrucţiuni pentru respectarea lor.

Se recomandă utilizatorilor să nu dezvăluie altor persoane informaţii care ar putea fi utilizate în scopuri periculoase lor.

Utilizatorii se obligă să respecte Politicile de utilizarea ale Platformei Office 365 impuse de Microsoft (http://privacy.microsoft.com/ro-ro/default.mspx)

5. Colaborarea.

Platforma Office 365 vine în sprijinul unor terţe părţi (cercetatori ai UO şi din alte institutii, întreprinderi, organizatii non-guvernamentale, etc.) care doresc să aiba acces la rezultatele obţinute în cadrul Platformei Office 365 prin activităţile sale. Colaborarea cu utilizatorii externi va avea loc numai în condiţiile în care aceştia vor da dovada de onestitate, credibilitate şi bune intenţii în solicitarea programelor de cercetare şi colaborare precum şi utilizarea în scopuri legale a rezultatelor acestor cercetări. Accesul utilizatorilor externi la resursele platformei va fi asigurat pe baza criteriilor de eligibilitate stabilite şi făcute public de membrii Office 365, în concordanţă cu misiunea şi scopul acesteia, pe criterii de performanţă şi echitate.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

6. Evitarea conflictelor de interese.

Activitatea pe Platforma Office 365 se va derula doar în condiţiile legii, în concordanţă cu misiunea declarată şi nu va susţine niciun scop ilicit al cercetării, formării şi difuzării informaţiei. Membrii şi utilizatorii săi vor evita orice situaţie în care obligaţiile profesionale ar putea fi compromise de urmărirea interesului personal. De asemenea, nu vor fi acceptate foloasele necuvenite obţinute prin acorduri cu terţe părţi care ar afecta integritatea şi prestigiului membrilor Platformei Office 365. Niciun membru al Platformei nu va accepta în nicio situatie colaborările neautorizate.

7. Promovarea onestităţii în susţinerea procesului de colaborare, comunicare, cercetare, învăţare şi evaluare.

Utilizatorii Platformei Office 365 vor respinge toate actele de difuzare de informaţii trunchiate sau false, denaturarea rezultatelor cercetărilor academice şi oricare altă manifestare de acest fel care ar putea altera misiunea şi rolul Platformei.

8. Grija faţă de bunurile Platformei.

Utilizatorii îsi asumă responsabilitatea respectării principiilor de conduită stabilite prin regulamentul de functionare şi codul de etică, grija faţă de bunurile Platformei, precum şi monitorizarea comportamentului persoanelor care participă în procesul de comunicare, colaborare, învăţare şi/sau evaluare a studenţilor pentru care au delegate responsabilităţi de coordonare şi instruire, astfel încât să fie protejate bunurile Platformei şi să fie utilizate în siguranţă.

Toţi utilizatorii Platformei Office 365 vor avea dreptul de a utiliza sistemul numai după o asumare prelabilă a prevederilor prezentului Ghid de norme etice privind utilizarea Platformei.

9. Promovarea transparentei activitatii Platformei Office 365.

Fiecare dintre utilizatorii interni va folosi platforma în folosul colectivităţii studenţeşti şi academice având la bază criteriile: confidenţialitate, transparenţă şi responsabilitate.

10. Respectarea principiului non-discriminarii.

Platforma Office 365 va putea fi folosită de toţi membrii abilitaţi de sistem, fără discriminare. Platforma este disponibilă pentru îmbunătăţirea procesului educaţional pentru oricare dintre facultăţile universitătii, indiferent de profil, scopul acesteia fiind promovarea formării studenţilor din orice domeniu şi de la oricare formă de învăţare universitară (cursuri de zi, învatamânt la distanţă sau frecvenţă redusă). De asemenea, accesul la utilizarea sa este oferit studenţilor şi tuturor categoriilor de cercetători şi formatori, indiferent de domeniul de specializare, vârstă, sex, etnie, apartenenţă politică, grad didactic sau funcţii ocupate în cadrul ierarhiei organizaţionale, în condiţiile în care activităţile prestate de aceştia vin în folosul întregii comunităţi academice şi a societăţii în ansamblul său.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

11. Preocuparea pentru formarea profesionala continua.

Toţi utilizatorii Platformei Office 365 vor depune toate eforturile pentru însuşirea modului de exploatare precum şi pentru asimilarea celor mai noi cunoştinţe care ar putea îmbunătăţi procesul de predare, formare, evaluare. Platforma Office 365 va fi adaptată în funcţie de evoluţiile pe plan mondial în acest domeniu.

12. Munca în echipă.

Platforma Office 365 promovează colaborarea şi munca în echipă pentru susţinerea activităţilor desfăşurate, evitându-se abuzul de putere din partea oricarui membru, orice decizie luându-se după consultarea membrilor şi a forurilor de decizie abilitate, în sprijinul întregii colectivităţi, cu scopul îmbunătăţirii şi perfecţionării.

13. Respectarea drepturilor de autor şi respingerea plagiatului.

Utilizatorii Platformei Office 365 se angajează să asigure respectarea drepturilor de autor, şi să respingă orice comportament ne-etic din partea utilizatorilor în sfera cercetării academice, cum ar fi plagiatul.

14. Responsabilitatea sociala a Platformei Office 365.

Membrii Platformei Office 365 îşi asumă respectarea prevederilor acestui Ghid de norme

APROBAT ÎN ŞEDINTA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 organizare si functionare a Serviciului Management Integrat IT

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Regulament de organizare si functionare a Serviciului Management Integrat IT

Misiune şi Obiective

Serviciul Management Integrat IT (SMIIT) are ca obiective:

- *Implementarea strategiei de dezvoltare permanentă, coerentă şi unitară a infrastructurii pentru tehnologiile informaționale şi de comunicații (ICT)* din Universitatea din Oradea, care să susțină performanța şi excelența în activitatea academică şi de cercetare din universitate;
- *Implementarea unui sistem informatic integrat* de gestionare a procesului educațional, prin automatizarea proceselor de prelucrare a informațiilor specifice din facultățile, centrele şi departamentele UO în vederea creşterii eficienței activității; se urmăreşte integrarea subsistemelor informatice dedicate procesului educațional, compartimentelor financiar-contabil şi de resurse umane şi altor departamente într-un sistem global de management universitar;
- *Asigurarea unor comunicații performante* printr-un acces fiabil la serviciile Internet pentru toate cadrele didactice, studenții şi personalul UO şi o continuă modernizare a facilităților Internet şi Intranet oferite de rețeua de comunicații a UO – UONet
- *Oferirea de facilități ICT* (tehnologia informației şi comunicațiilor) performante pentru studenții, cadrele didactice şi angajații UO referitoare la accesul, prelucrarea şi comunicarea informațiilor relevante pentru fiecare categorie de utilizatori din UO;
- *Oferirea de servicii electronice* accesibile şi eficiente de informare a comunității publice, asupra programelor academice şi a facilităților educaționale ale UO.

TITLUL 1 - DISPOZIȚII GENERALE

Art. 1 Serviciul Management Integrat IT (SMIIT), este constituit prin decizia rectorului, fiind aflat sub directa sa coordonare şi implementeze strategiile UO de introducere a tehnologiilor moderne de comunicație în învățământ, cercetare şi administrație.

Art. 2 Serviciul Management Integrat IT (SMIIT) este o structura de specialitate cu rol de execuție, coordonare şi consultanță ce deserveşte toate facultățile, departamentele, centrele şi campusul UO în vederea implementării facilităților de tehnologia informației şi comunicațiilor – ICT necesare pentru desfăşurarea unei activități eficiente.

Art. 3 Universitatea din Oradea asigură instruirea personalului şi a studenților la un nivel care să permită fructificarea oportunităților electronice de informare şi comunicare.

Art. 4 Serviciul Management Integrat IT (SMIIT), conform organigramei aprobate de Senat, este subordonat Rectorului.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

TITLUL 2 – ORGANIZAREA, MANAGEMENTUL ŞI ACTIVITATEA SERVICIULUI

Capitolul 1- Structura şi organizarea Serviciului

Art. 5 Serviciul Management Integrat IT (SMIIT) urmăreşte aplicarea unei politici unitare şi coerente privind gestionarea eficientă a infrastructurii pentru tehnologiile informaționale şi de comunicații (infrastructura ICT) din Universitatea din Oradea.

Art. 6 Organizarea Serviciului Management Integrat IT (SMIIT) şi schema posturilor din serviciu trebuie să asigure implementarea strategiilor de dezvoltare ICT ale UO.

Capitolul 2 - Integrarea în organigrama UO şi colaborări ale Serviciului

Art. 7 Serviciul Management Integrat IT (SMIIT) este un serviciu al UO subordonat Rectorului.

Art. 8 Serviciul Management Integrat IT (SMIIT) asigură implementarea strategiilor ICT din UO în toate facultățile, departamentele, centrele, structurile şi campusul UO.

Art. 9 Serviciul Management Integrat IT (SMIIT) colaborează cu departamentele de profil Calculatoare si Tehnologia Informatiei, respectiv de Informatica din UO, cu departamente similare din alte instituții academice, cu mediul de business ICT în vederea perfecționării facilităților ICT oferite în cadrul UO şi de către UO pentru comunitatea publică.

Capitolul 3 - Managementul Serviciului

Art. 10 Serviciul Management Integrat IT (SMIIT) este condus de directorul Serviciului Management Integrat IT (SMIIT). Directorul Serviciului Management Integrat IT (SMIIT) este subordonat Rectorului. El este ajutat in activitate de un Consiliu al Serviciului ce include coordonatorii operativi ai compartimentelor din structura serviciului la care se adaugă un anumit număr de cadre didactice de specialitate angajate □n departamentele de profil ale universității. Directorul este desemnat prin concurs public/numit temporar, pentru coordonarea intregii activitati, prin decizia Rectorului. Atribuțiile directorului Serviciului Management Integrat IT (SMIIT) sunt:

- Elaborează strategia ICT în UO, în acord cu strategiile generale de dezvoltare ale UO stabilite de Senatul UO, o supune spre avizare Consiliului de Administrație şi aprobare Senatului Universității şi asigură implementarea acestei strategii;
- Coordonează activitatea Serviciului de Management Integrat IT;
- Coordonează modernizarea serviciilor ICT din cadrul rețelei de comunicații digitale UONet şi propune Conducerii Universității, strategii de dezvoltare şi modernizare a rețelei de comunicații digitale UONet;
- Asigură managementul proiectelor informatice din cadrul Serviciului Management Integrat IT (SMIIT) şi a proiectelor informatice realizate la nivelul UO;
- Coordonează asigurarea accesului la facilități ICT şi sisteme informatice dedicate pentru toți studenții, cadrele didactice şi angajații UO, în acord cu obiectivele activității acestora;
- Urmăreşte, în numele Rectorului, respectarea principiilor, politicii şi regulamentelor de membru RoEduNet, definite conform Regulamentului de Funcționare al Infrastructurii de Comunicații de Date RoEduNet, aprobat prin OMEN nr.3704 din 26.04.2000;

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- Coordonează elaborarea politicii de securitate a rețelei de comunicații digitale a UO - UONet, conform Regulamentului menționat, inclusiv politica de acces la serviciul de INTERNET a personalului UO, a studenților în procesul didactic şi a studenților din campusul universitar şi o supune spre aprobare. Aceste reglementări sunt detaliate în Politica de securitate a rețelei de comunicații digitale UONet care vor fi afişate pe site-ul universității.
- Coordonează proiecte de modernizare a infrastructurii de comunicații, proiecte de implementare a unor aplicații destinate procesului educațional şi proiecte academice de cercetare/colaborare încheiate în numele Universității şi realizate în comun de mai multe facultăți;
- Elaborează propuneri către Conducerea UO, pentru respectarea standardelor, a bunelor practici şi gestionarea eficientă a echipamentelor de comunicații şi IT din punct de vedere al utilizării, întreținerii, dezvoltării;
- Colaborează cu compartimentele tehnic / achiziții ale UO şi cu partenerii IT în vederea dezvoltării rețelei de comunicații digitale şi a facilităților ICT oferite în cadrul UO;
- Avizează specificațiile tehnice şi rapoartele de evaluare tehnică a ofertelor pentru achizițiile de echipamente de tehnică de calcul şi comunicații, licențe software, pentru lucrări de dezvoltare a infrastructurii ICT şi service la tehnica de calcul de la UO;
- Confirmă realizarea obligațiilor contractuale pentru furnizorii de servicii ITC şi furnizorii de service la echipamentele de calcul şi la infrastructura ICT ai UO;
- Propune şi implementează organizarea site-ului principal al UO www.uoradea.ro , supervizat de Consiliul de Administratie;
- Supervizează proiectarea sistemului de pagini Web şi a ierarhiilor de protecție aferente paginilor facultăților / departamentelor / centrelor UO;
- Elaborează Regulamentul de funcționare al Serviciului de Management Integrat IT şi îl supune spre aprobare Senatului Universității din Oradea;
- Propune Conducerii Universității şi atunci când este cazul, sancționarea utilizatorilor care încalcă prevederile angajamentului de membru al rețelei de comunicații digitale UONet, cu respectarea prevederilor Cartei Universitare şi ale LEN.

Capitolul 4 - Strategiile Serviciului

Serviciul Management Integrat IT (SMIIT):

Art. 11 Asigură mecanismele de implementare şi dezvoltare a facilităților ICT în cadrul UO în scopul creşterii eficienței în domeniile gestiunii procesului educațional şi al managementului academic.

Art. 12 Urmăreşte îmbunătățirea facilităților ICT oferite tuturor utilizatorilor din cadrul UO (studenți, cadre didactice, personal administrativ, management academic şi administrativ), în acord cu obiectivele fiecărei categorii de utilizatori.

Art. 13 Propune direcțiile de dezvoltare şi modernizare a sistemelor informatice utilizate în cadrul UO.

Art. 14 Asigură dezvoltarea şi modernizarea rețelei de comunicații digitale UONet şi a serviciilor de comunicații oferite în cadrul acesteia.

Art. 15 Asigură evaluarea permanentă a vulnerabilităților potențiale ale rețelei de date la accesul neautorizat, expunerea la viruşi şi alte amenințări de pe INTERNET şi elaborează soluții pentru minimizarea acestor riscuri într-o manieră optimă în raport de cost-eficiență.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Art. 16 Contribuie la promovarea prin mijloace electronice a programelor academice şi activităţii UO în comunitatea publică.

Art. 17 Colaborează cu departamentele de profil din UO şi cu structuri similare din alte instituţii academice în scopul dezvoltării facilităţilor ICT oferite.

Capitolul 5 - Activitatea şi responsabilităţile Serviciului

Art. 18 **Serviciul Management Integrat IT (SMIIT) asigură:**

- administrarea şi securitatea nodurilor centrale de comunicaţii şi coordonează administrarea serverelor de comunicaţii din facultăţile, departamentele, centrele şi campusul UO;
- administrarea conexiunilor din nivelul superior al reţelei de comunicaţii digitale UONet şi integrarea acesteia în Internet (în principal, prin reţeaua educaţională naţională RoEduNet);
- accesul fiabil la serviciile Internet şi aplicaţiile bazate pe acestea pentru toate cadrele didactice, studenţii şi personalul UO;
- accesul studenţilor, cadrelor didactice şi personalului UO la diverse aplicaţii informatice dedicate, cu acces distribuit, bazat pe accesul în reţea;
- dezvoltarea, modernizarea şi securitatea reţelei de comunicaţii digitale UONet în conformitate cu **Politica de securitate a reţelei de comunicaţii digitale UONet** şi **Politica de securitate a reţelei de comunicaţii digitale din Campusul UO**;
- dezvoltarea de facilităţi electronice de promovare a programelor academice ale UO în comunitatea publică prin: site-ul principal www.uoradea.ro;
- funcţionalitatea (administrare servere şi aplicaţii) pentru programele informatice utilizate curent în administraţie şi pentru Sistemul Informatic Integrat care se va implementa;
- elaborarea de propuneri către Conducerea UO, pentru respectarea standardelor, a bunelor practici şi gestionare eficientă a echipamentelor de comunicaţii şi ICT din punct de vedere al utilizării, întreţinerii, dezvoltării;
- accesul la serviciile de comunicare telefonică pentru personalul UO pe telefonia fixă şi mobilă, conform cu bugetele aprobate în acest scop de Conducerea Universităţii.

Art. 19 Serviciul Management Integrat IT (SMIIT) asigură administrarea serverelor pentru sistemele informatice destinate procesului educaţional şi proiecte academice de cercetare/colaborare încheiate în numele Universităţii şi realizate în comun de mai multe facultăţi.

Art. 20 Serviciul Management Integrat IT (SMIIT) asigură administrarea tehnologiilor de tip *eLearning* (platforme software, sisteme de videoconferinţă) implementate pe infrastructura ICT de la Universitatea din Oradea.

Art. 21 Serviciul Management Integrat IT (SMIIT) colaborează în vederea realizării specificaţiilor pentru configuraţiile hard şi soft necesare accesului performant al utilizatorilor la facilităţile acordate prin sistemele informatice distribuite ale UO.

Art. 22 Serviciul Management Integrat IT (SMIIT) urmăreşte derularea contractelor de service cu terţi pentru echipamentele de calcul şi infrastructura ICT.

Art. 23 Serviciul Management Integrat IT (SMIIT) asigură coordonarea cadrelor de specialitate informatică din servicii şi departamente.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Capitolul 6 - Angajaţii Serviciului

Art. 24 Angajaţii Serviciul Management Integrat IT (SMIIT) ocupă posturile din schema Serviciului şi îşi desfăşoară activitatea în conformitate cu reglementările în vigoare legate de politica de resurse umane din UO şi cu legislaţia muncii din România.

Art. 25 Serviciul Management Integrat IT (SMIIT) asigură implementarea strategiilor ICT din UO în toate facultăţile / departamentele / centrele UO prin asistenţă directă acordată de angajaţii Serviciului şi prin intermediul informaticienilor şi inginerilor de sistem angajaţi în facultăţi / departamente / centre.

Art. 26 Coordonarea profesională IT a personalului IT angajat în facultăţile şi departamentele UO este realizată prin intermediul Serviciului Management Integrat IT (SMIIT). Personalul IT din facultăţile, departamentele şi centrele UO sau persoanele desemnate din facultăţi / departamente / centre să îndeplinească aceste atribuţii trebuie să respecte deontologia profesională IT, prevederile prezentului regulament, referitoare la responsabilităţile angajaţilor şi prevederile legale din domeniu.

Art. 27 Angajaţii Serviciului Management Integrat IT (SMIIT) acordă, la cerere, asistenţă profesională personalului IT din facultăţi / departamente / centre oricând este necesar, pentru îndeplinirea atribuţiilor de serviciu ale acestora.

Art. 28 Inginerii de sistem/ analistii asigură, pentru toate cadrele didactice, studenţii şi personalul facultăţilor / departamentelor / centrelor, accesul la resurse informaţionale şi programe în reţelele locale şi accesul la serviciile Internet prin intermediul serverelor de comunicaţii din UO.

Art. 29 Atribuţiile personalului IT din UO [1]:

- răspunde de funcţionarea eficientă a reţelelor locale şi de buna integrare a acestora în reţeaua UONet;
- asigură instalarea, configurarea, întreţinerea şi modernizarea fizică a calculatoarelor şi echipamentelor de conectare din reţeaua locală administrată;
- asigură implementarea unui soft adecvat, respectând contractele de licenţiere ale UO şi facultăţilor / departamentelor / centrelor, prin care să se ofere, în condiţii de eficienţă şi securitate, accesul tuturor utilizatorilor la resursele fizice şi logice ale reţelei;
- asigură, pentru toate cadrele didactice, studenţii şi personalul universităţii, accesul la resurse informaţionale şi programe în reţelele locale şi accesul la serviciile Internet prin intermediul serverelor de comunicaţii din facultăţi (aflate sub administrarea inginerilor/administratorilor structurilor respective);
- asigură prin intermediul inginerilor/administratorilor structurilor respective configurarea necesară în sistemele de operare din reţelele locale pentru o funcţionare optimă a sistemelor informatice ale UO.

Capitolul 7 - Drepturile şi obligaţiile angajaţilor

Art. 30 Angajaţii Serviciului Management Integrat IT (SMIIT) beneficiază de:

- drepturile de muncă şi salariale prevăzute de legislaţia muncii (sectorul bugetar);

[1] Este vorba despre cei ce gestioneaza retelele locale

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- mecanismele rezultate din politica de resurse umane a UO şi din strategia UO de dezvoltare a domeniului IT.

Art. 31 Angajaţii Serviciului Management Integrat IT (SMIIT) au obligaţia:

- respectării prevederilor legale cu privire la statutul şi gestionarea informaţiilor electronice,
- respectării deontologiei profesionale în domeniul ICT;
- asigurării securităţii reţelei de comunicaţii digitale UONet, a informaţiilor electronice stocate, prelucrate şi transmise în şi din cadrul reţelei de comunicaţii digitale UONet, precum şi prin intermediul sistemelor informatice ale UO;
- păstrării confidenţialităţii informaţiilor electronice gestionate ca atribuţii de serviciu.
- Să răspundă prompt □n termen de maxim 2 zile la solicitările interne date in cadrul serviciului făcute telefonic, prin email sau pentru situatiile in care nu functioneaza emailul, comunicarea se va face prin adresă scrisă. In situatia □n care se cere răspuns scris angajatii serviciului au obligaţia să răspundă □n scris
- Să comunice scris şi argumentat rezoluţiile negative date solicitărilor scrise primite cu privire la activităţi solicitate □n cadrul sarcinilor ce le revin

TITLUL 3 – FACILITĂŢI ICT OFERITE UTILIZATORILOR

Capitolul 8 - Statutul şi securitatea informaţiilor şi aplicaţiilor informatice din UO şi reţeaua UONet

Art. 32 Serviciul Management Integrat IT (SMIIT) urmăreşte asigurarea cât mai extinsă, accesibilă şi eficientă a facilităţilor şi serviciilor ICT pentru toţi utilizatorii din cadrul UO (studenţi, cadre didactice, personal administrativ, management academic şi administrativ) în vederea asistării electronice a activităţii acestora în cadrul UO şi în acord cu obiectivele fiecărei categorii de utilizatori. Astfel, se pun la dispoziţia utilizatorilor: servicii Internet de informare şi comunicare electronică, sisteme informatice implementate în cadrul UO, contracte de licenţiere software, alte facilităţi ICT.

Art. 33 Reţeaua UONet este integrată în reţeaua naţională educaţională RoEduNet. Ca membru al comunităţii RoEduNet, UO respectă în cadrul reţelei de comunicaţii digitale UONet statutul şi regulamentul de funcţionare al RoEduNet, aprobat prin OMEN 3704 / 26.04.2000 (http://www.roedu.net/regrom.html)

Art. 34 Informaţiile publicate electronic de către UO pe site-ul propriu www.uoradea.ro, în subdomeniile acestuia şi pe platformele de lucru ale UO, sunt proprietate a UO. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către UO în beneficiul comunităţii publice, în scop de informare asupra programelor academice şi a activităţii UO.

Informaţiile depuse pe site-urile publice ale facultăţilor / departamentelor / centrelor UO / structurilor UO aparţin facultăţilor / departamentelor / centrelor / structurilor respective ca şi subunităţi organizatorice ale UO, iar informaţiile din conturile atribuite utilizatorilor reţelei de comunicaţii digitale UONet aparţin acestora, cu implicaţiile legale aferente.

Orice utilizare a informaţiilor de pe site-urile publice ale UO în domeniul uoradea.ro de către persoane particulare sau organizaţii în alte scopuri decât cele în care au fost oferite, se face pe

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 4.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

propria răspundere a acestora. Într-o asemenea eventualitate, UO îşi rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.
Art. 35 Domeniul electronic uoradea.ro şi subdomeniile acestuia sunt gestionate de UO ca domenii proprii, în conformitate cu înregistrarea corespunzătoare a UO ca proprietar al acestui domeniu la autoritatea românească în materie de nume de domenii (ROTLD). Drepturile de utilizare ale domeniului uoradea.ro sunt rezervate pentru UO.

Art. 36 Informaţiile electronice gestionate în sistemele informatice interne ale UO sunt proprietate a UO şi au caracter privat, intern UO. Anumite informaţii pot fi puse la dispoziţia diverselor categorii de utilizatori din UO (studenţi, cadre didactice, management academic, management administrativ), spre beneficiul acestora, prin mecanisme electronice adecvate, în acord cu necesităţile şi drepturile electronice ale categoriilor de utilizatori. Orice tentativă de violare a sistemelor de drepturi acordate utilizatorilor sistemelor informatice din cadrul UO sau a securităţii sistemelor informatice respective va fi considerată tentativă de violare a securităţii reţelei de comunicaţii digitale UONet şi va fi tratată conform Art. 38 din prezentul regulament.

Art. 37 Facilităţile hard şi soft ale reţelei de comunicaţii digitale UONet sunt puse la dispoziţia utilizatorilor din cadrul UO (studenţi, cadre didactice, angajaţi), spre beneficiul acestora, în scopuri academice, de cercetare sau în vedea realizării atribuţiilor de serviciu, în conformitate cu angajamentul utilizatorului reţelei de comunicaţii digitale UONet, odată cu semnarea unui angajament (Anexa 1 – angajamentul utilizatorului reţelei de comunicaţii digitale UONet). Cu referire la studenti acestia vor semna angajamentul odata cu semnarea contractului de studii anual, iar cadrele didactice vor semna prin intermediul decanatelor si personalul TESA vor semna prin Departamentul Resurse Umane.

Art. 38 Orice utilizare neconformă cu statutul de utilizator al reţelei UONet sau orice tentativă de violare a securităţii reţelei de comunicaţii digitale UONet, a unor sisteme informatice din UO sau din afara UO, va atrage măsuri de blocare parţială sau totală a accesului acelui utilizator la facilităţile electronice oferite în cadrul reţelei de comunicaţii digitale UONet. Eventuale acţiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea reţelei Internet vor fi tratate în acord cu legislaţia în vigoare.

Art. 39 Respectarea legalităţii şi eticii proprietăţii informaţiilor în accesarea şi utilizarea acestora se va face de către toţi utilizatorii reţelei de comunicaţii digitale UONet, în cadrul sistemelor interne UO şi în Internet .

Capitolul 9 - Drepturile şi obligaţiile utilizatorilor

Art. 40 Utilizatorii reţelei de comunicaţii digitale UONet au dreptul de a beneficia de:

- facilităţile şi serviciile ICT oferite lor de către Serviciul Management Integrat IT (SMIIT) în acord cu statutul academic al reţelei de comunicaţii digitale UONet,
- serviciile Internet de informare şi comunicare electronică oferite în cadrul reţelei de comunicaţii digitale UONet,
- acces la informaţii şi servicii IT oferite prin intermediul sistemelor informatice implementate în cadrul UO, în acord cu drepturile fiecărei categorii de utilizatori,
- contractele de licenţiere software ale UO în derulare, în acord cu prevederile acestora.

Art. 41 Utilizatorii reţelei de comunicaţii digitale UONet au următoarele obligaţii:

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- a utiliza, în cadrul rețelei de comunicații digitale UONet, serviciile Internet de informare şi comunicare electronică în acord cu statutul academic al rețelei (Anexa 1) şi în condiții de legalitate privitoare la accesul la informații şi produse soft,
- luarea la cunoştință şi semnarea angajamentului utilizatorului rețelei de comunicații digitale UONet,
- a accesa / gestiona, în cadrul rețelei de comunicații digitale UONet, informații publice pe Internet sau informații din cadrul rețelei de comunicații digitale UONet în acord cu şi cu drepturile de acces asupra acestor informații. Eventuale tentative de accesare a unor informații pentru care utilizatorii care nu au drept de acces vor fi tratate conform art. 39 din prezentul regulament.
- a folosi în cadrul rețelei de comunicații digitale UONet soft-uri asupra cărora au drept de utilizare, în acord cu clauzele contractelor de licențiere software ale UO, ale facultăților sau departamentelor care contractează soft-uri specifice.
- a respecta drepturile fiecărei categorii de utilizatori în folosirea facilităților IT puse la dispoziția utilizatorilor prin intermediul sistemelor informatice implementate în UO; eventuale tentative de utilizare frauduloasă a acestor facilități electronice vor fi tratate conform art. 38 din prezentul regulament.

Capitolul 10 - Structurarea responsabilităților IT în organigrama UO

Art. 42 Serviciul Management Integrat IT (SMIIT), ce functioneaza conform organigramei din Anexa 2, gestionează:

- site-ul principal al UO uoradea.ro, site-urile de email pentru cadre didactice, personal administrativ şi studenți,
- sistemele informatice implementate în cadrul UO şi / sau destinate tuturor facultăților / departamentelor / centrelor / structurilor şi campusului UO.

Art. 43 Organizarea fluxului de informații necesar pentru actualizarea site-ului principal al UO: www.uoradea.ro este coordonată, pe domeniile de competență, de prorectori.

Art. 44 Facultățile pot gestiona, prin intermediul responsabililor numiți în fiecare facultate, site-ul propriu

Art. 45 Serviciul Management Integrat IT (SMIIT) asigură administrarea nivelului superior al rețelei de comunicații digitale UONet şi a serverelor de comunicații ale UO

Art. 46 Inginerii de sistem / administratori de rețea din Serviciul Management Integrat IT (SMIIT) vor realiza administrarea rețelelor locale ale serviciului, care presupune:

- instalarea, configurarea, întreținerea şi modernizarea fizică a calculatoarelor şi echipamentelor de conectare,
- instalarea unui soft de bază adecvat, prin care să se ofere, în condiții de eficiență şi securitate, accesul tuturor utilizatorilor la resursele fizice şi logice ale rețelei. Se vor utiliza softuri pentru care există drepturi de utilizare prin contractele de licențiere ale UO sau contracte de licențiere specifice în cazul unor soft-uri dedicate, necesare în anumite facultăți / departamente.

Art. 47 Serviciul Management Integrat IT (SMIIT) asigură implementarea de sisteme informatice în facultăți / departamente / centre / structuri. Prn intermediul personalului responsabil la nivelul structurilor, Serviciul Management Integrat IT (SMIIT) asistă utilizatorii, în utilizarea acestor sisteme, prin asistența directă şi punerea la dispoziție a unor documentații accesibile.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Art. 48 Introducerea şi actualizarea bazelor de date gestionate de sistemele informatice instalate în facultăţi / departamente/ centre / structuri (Art. 36, Art. 37), prin interfeţe utilizator accesibile, precum şi completitudinea şi acurateţea acestor baze de date sunt responsabilităţi ale utilizatorilor sistemelor respective.

Art. 49 Informaţiile bazelor de date gestionate de sistemelor informatice din facultăţi / departamente (Art. 36, Art. 37) aparţin facultăţilor / departamentelor, respectiv UO, şi pot fi accesate de categorii de utilizatori autorizaţi ai sistemelor informatice care gestionează bazele de date respective în funcţie de drepturile acordate acestora, şi în condiţiile de securitate stabilite la Art. 36, Art. 37 din prezentul regulament.

Art. 50 Responsabilitatea asigurării securităţii în subreţelele (căminele) din campusul universitar al UO aparţine Serviciul Management Integrat IT (SMIIT). În cazul apariţiei unor fraude grave pe Internet produse din subreţelele respective, UO îşi rezervă dreptul de a sista serviciile de comunicaţii oferite căminului până la clarificarea incidentului, având în vedere că în Internet subreţelele din cămine sunt catalogate ca aparţinând reţelei UO.

Capitolul 11 – Dispoziţii finale şi tranzitorii

Art. 51 Aprobarea regulamentului de funcţionare a Serviciul Management Integrat IT (SMIIT) al UO se face de către Senatul UO.

Art. 52 Orice dispoziţie contrară acestui regulament, din dispoziţii anterioare referitoare la activitatea de informatizare-comunicaţii din UO, se abrogă o dată cu aprobarea prezentului regulament. Dispoziţiile acestui Regulament pot fi modificate cu avizul Serviciul Management Integrat IT (SMIIT), la propunerea Consiliului de Administratie şi cu aprobarea Senatului UO.

Art. 54 Solicitarile structurilor UO la nivelul Serviciului Management Integrat IT se vor adresa prin email la adresa gbotau@uoradea.ro si se va depune o adresa scrisa la Sediul serviciului (Biblioteca Noua etaj II)

Art. 54 Modificarile la prezentul Regulament se vor efectua de catre Directorul serviciului Management Integrat IT.

Referinţe

1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.dict.UO.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ANGAJAMENT

Subsemnatul, _____ cadru didactic/cercetător/personal de administrație / student al Universității din Oradea, la facultatea/departamentul: _____, devenind utilizator al rețelei de comunicații digitale UONet, am luat la cunoștință și voi respecta următoarele principii de utilizare a rețelei:

1. Comunicarea în INTERNET este folosită numai în scopuri educaționale sau de cercetare, nu în scopuri comerciale, politice, de divertisment etc. Spiritul INTERNET presupune dialoguri într-un stil academic, caracterizat prin decență, amabilitate și bunăvoință și exclude comportamentul antisocial.

2. Fiecare utilizator are acces la rețea □i este direct responsabil pentru facilitățile utilizate din contul lui, fiind singurul care poate beneficia de ele, datorită drepturilor asociate contului de utilizator. Dacă utilizatorul constată/ bănuiește că i-a fost descoperită parola, o va schimba imediat; dacă fenomenul se repetă, va anunța administratorul de sistem/rețea. Utilizatorii standard nu beneficiază de drept de administrare rețea.

3. Serviciile Internet se utilizează în acord cu etica Internet și principiile enunțate la punctul 1. Este interzisă violarea sistemelor de protecție a serverelor din rețeaua proprie sau a oricărui server aflat în rețeaua INTERNET.

4. Programele și aplicațiile informatice din cadrul rețelei de comunicații digitale UONet se utilizează în scopuri didactice și de cercetare, nu în scopuri comerciale, politice, de divertisment (jocuri, site-uri XXX).

5. Se utilizează numai softuri licențiate, în acord cu contractele de licențiere ale UO și ale facultăților. Eventuala prezență a unui soft nelicențiat în directoarele utilizatorului cade în răspunderea acestuia.

6. Pentru a asigura o funcționare optimă a serviciului de email, utilizatorii se obligă să mențină în directoarele proprii pe serverul de email numai mesajele strict necesare, în limita spațiului alocat. La cererea administratorului rețelei, utilizatorii vor elibera (părți din) spațiile de pe server pe care le ocupă.

7. În utilizarea sistemelor informatice implementate în cadrul UO diverselor categorii de utilizatori, spre beneficiul acestora, (studenți, cadre didactice, personal administrativ, management), se vor respecta drepturilor de acces acordate. Orice tentativă de violare a securității sistemelor respective va atrage blocarea totală sau parțială a accesului la facilitățile oferite de sistemele respective.

8. Semnarea acestui document implică folosirea responsabilă a echipamentelor, facilităților și resurselor puse la dispoziție. Nu se vor deteriora/distruge echipamentele, resursele oferite de sistem, resursele aparținând altor utilizatori.

În cazul nerespectării celor de mai sus, se vor lua măsuri de blocare totală sau parțială a accesului la facilitățile rețelei de comunicații digitale UONet.

Data:_____ Semnătura

Nume_user :_____

Adresa E-mail :_____

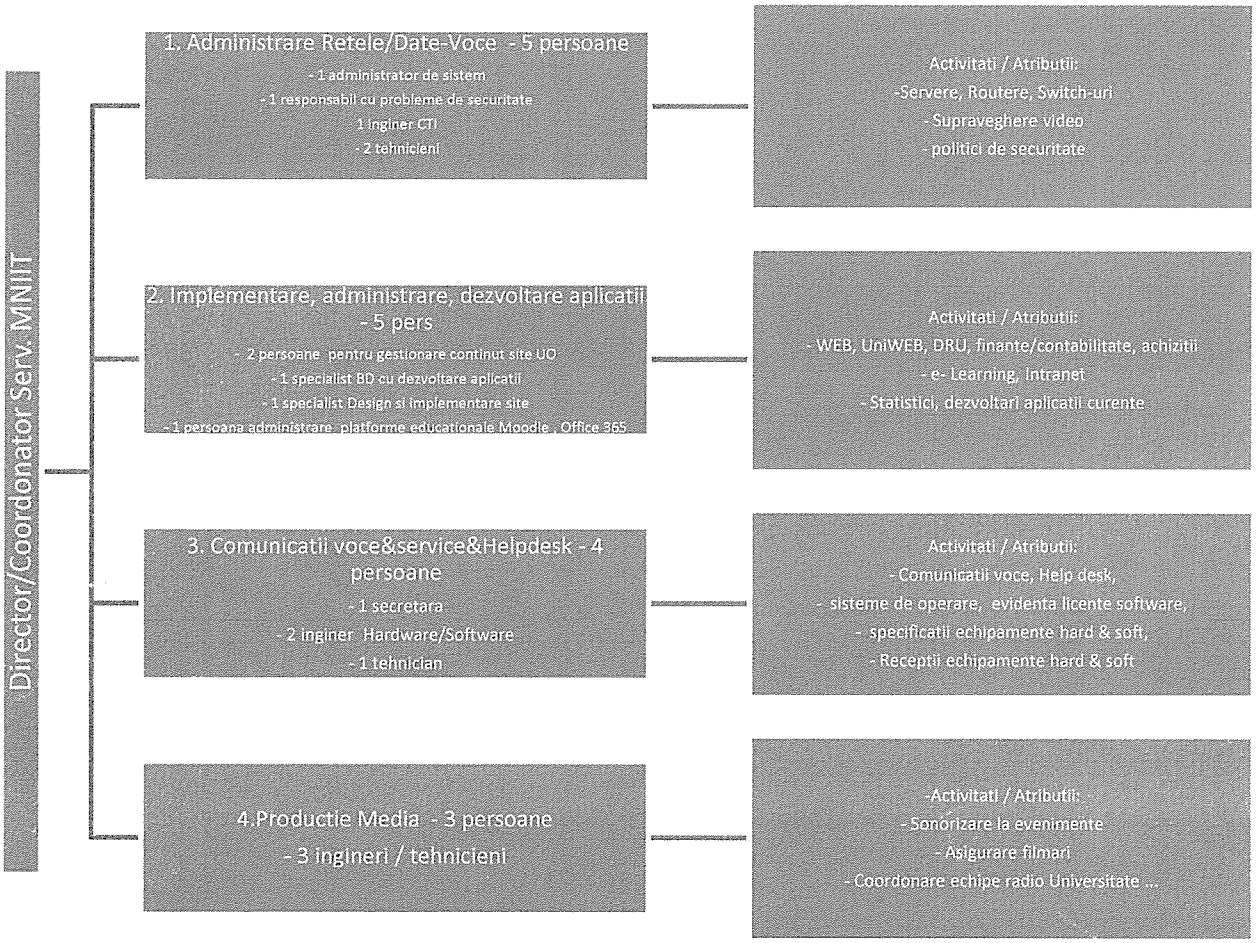
APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI CERCETĂRII TINERETULUI SI SPORTULUI
UNIVERSITATEA DIN ORADEA
Adresa: Str. Universității nr.1, Oradea, România
Telefon: +40 259 432830 Fax: +40 259 432789
E-mail: rectorat@uoradea.ro Pagina web: www.uoradea.ro
CUI 4287939

Nr. _____

Anexa 2

Organigrama serviciului:



APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Campusului Universității din Oradea

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 12.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Politica de securitate a Campusului Universității din Oradea

Condițiile în care Universitatea din Oradea (abreviată UO) furnizează serviciul de acces la rețeaua Internet şi serviciile asociate acestuia, denumite generic „Serviciul" Campusului Universitar, sunt următoarele[1]:

I. UO in calitate de furnizor se obliga:

1. să asigure accesul la Serviciu de date tuturor utilizatorilor din Campusul Universitar;

2. să pună la dispoziție un hub central;

3. să anunțe din timp eventualele întreruperi in furnizarea Serviciului de Date.

II. Utilizatorul in calitate de client are următoarele drepturi şi responsabilități:

1. Utilizatorul are dreptul să se conecteze in orice punct al rețelei beneficiind de serviciile de bază, orice acces suplimentar se face pe bază de cerere către conducerea Serviciului Management Integrat IT;

2. Utilizatorul are obligația de a pune la dispoziția furnizorului adresa Mac a plăcii de retea cu care se va face conectarea la internet;

3. Utilizatorul nu are permisiunea de a utiliza Serviciul pentru a transmite, a copia, a posta, a distribui, a reproduce, a utiliza, a încărca sau a prelucra in orice alt mod materiale:

a) ilegale, obscene, vulgare, calomniatoare, amenințătoare, abuzive, materiale care îndeamnă la ura rasiala, etnica sau sunt in orice alt mod defăimătoare;

b) pentru care nu are dreptul legal de transmitere, reproducere sau difuzare, sub orice sistem juridic, românesc sau străin;

c) care conțin viruşi sau orice alt tip de cod, fişiere, sau programe care sunt create să distrugă, întrerupă sau să limiteze funcționarea oricărui alt software, componente hardware sau echipament de telecomunicații;

4. Utilizatorul nu are dreptul:

a) de a utiliza serviciul in scopul instigării la, lansării sau coordonării de atacuri informatice de orice tip împotriva oricărui sistem sau utilizator de Internet sau de pe alte rețele conectate sau nu la Internet, prin metode wired, wireless sau in alte tehnologii

[1] Furnizarea Serviciului este condiționată de acceptarea în întregime a prevederilor acestei Politici.

APROBAT ÎN ŞEDINTA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. ŞORIN CURILĂ

existente sau viitoare, incluzând (fără a se limita la) atacuri *Denial of Services DoS sau Distributed DoS*; trimiterea de mesaje *spam*; furt de identitate electronică sau obținerea de foloase necuvenite prin exploatarea vulnerabilităților sistemelor *phishing; pharming; click fraud; spyware; keylogging; sniffing;*

b) de a utiliza adresa de IP primită ca urmare a utilizării Serviciului, in programe rulate pe un calculator de orice tip cu scopul de a obține informații / rapoarte de la alte calculatoare utilizate pentru scopuri ilegale, cum ar fi *spamming* sau alte acțiuni ilegale.

III. Responsabilitatea pentru conținutul documentelor.

Utilizatorul este în întregime responsabil pentru toate materialele pe care le încarcă, reproduce, pune la dispoziție în mod public.

Pentru toate informațiile, datele, software-ul, precum şi orice alte materiale incluzând (fără a se limita la) muzică, sunet, fotografii, grafice, materiale video, mesaje, indiferent dacă au fost afişate în mod public sau transmise / accesate individual, prin intermediul Serviciului, persoana care a fost sursa unor astfel de materiale este responsabilă.

IV. Conexiunea la alte Rețele

UO nu este responsabil pentru situațiile in care accesul Utilizatorului la anumite domenii de Internet nu este permis (urmare a includerii IP-ului Utilizatorului in anumite liste negre („black lists") sau pentru orice alte motive.

V. Securitatea sistemului şi a rețelei.

Utilizatorul nu are voie să încalce sau să încerce să încalce securitatea rețelei şi a Serviciilor prin:

1. încercarea de a proba, scana sau testa vulnerabilitatea unui sistem sau a unei rețele sau de a încălca securitatea acestuia / acesteia sau măsurile de autentificare fără a fi autorizat in mod corespunzător;

2. încercarea de a interfera cu scopul de a întrerupe sau de a face inutilizabil Serviciul de către un alt utilizator, gazdă sau rețea inclusiv, dar fără a se limita la, mijloace de supraîncărcare, "*flooding*" sau "*crashing*";

3. contrafacerea oricărui "header" TCP/IP sau a oricărei părți din informația cuprinsă în acesta. Pentru protejarea rețelei, a resurselor furnizorului Internet, precum şi a celorlalți clienți, în cazul unor atacuri de tip "*Denial-of-Service*" având ca țintă adrese Internet alocate

UO nu monitorizează comunicațiile Utilizatorului în scopul verificării conformității cu prezenta Politică. Totuşi, atunci când UO deține informații cu privire la activități ale Utilizatorului contrare celor de mai sus, poate lua orice masuri pe care le consideră necesare în vederea încetării acestor activități, incluzând (fără a se limita la) eliminarea informației, blocarea accesului la Internet, rezilierea Contractului de furnizare servicii şi refuzul ulterior de a încheia contracte cu Utilizatorul. Utilizatorul este obligat să permită reprezentanților UO accesul la calculator pentru a verifica respectarea de către Utilizator a dispozițiilor acestei Politici.

VI. Limitarea răspunderii

Utilizatorul declara in mod expres că înțelege şi este de acord cu următoarele:

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 14.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

1. UO nu oferă nicio garanție că: Serviciul va împlini toate cerințele Utilizatorului; Serviciul va fi furnizat neîntrerupt, la timp, sigur sau fără erori; orice eroare de program va fi corectată;

2. Exceptând dispozițiile contrare din Contract, UO nu își asumă nicio responsabilitate privind orice fel de pagubă de orice natură provocată de Utilizator prin intermediul sau cu ajutorul IP-ului obținut in momentul conectării. UO nu este responsabil de nici-un fel de daune directe, indirecte, accidentale sau pentru comunicații întrerupte, pierderi de date sau profituri cauzate de utilizarea Serviciului. UO nu va fi răspunzător pentru nici-un fel de pagube de orice natură suferite de Utilizator sau orice terță parte, care rezultă în totalitate sau în parte din exercitarea de către UO a drepturilor sale în baza acestei Politici. UO nu va fi răspunzător, fără ca enumerarea sa fie limitativă, pentru alterarea şi/sau securitatea informațiilor care tranzitează Internetul;

3. Utilizatorul este de acord să exonereze de răspundere şi să despăgubească UO atât cu privire la orice pretenție ridicata de către un terț, rezultată din Utilizarea Serviciului sau a rețelei de comunicații a UO şi a Internetului de către Utilizator, cât şi cu privire la orice pierdere (directă, indirectă, pe cale de consecință sau de alta natură), costuri, acțiuni, procese, pretenții, cheltuieli (inclusiv cheltuieli de judecată) sau alte răspunderi, suferite in vreun fel sau provocate ca urmare a încălcării sau ignorării de către Utilizator a acestei Politici.

4. Orice material descărcat sau obținut în alt fel prin utilizarea Serviciului se află astfel la discreția şi poate fi folosit doar pe riscul propriu al Utilizatorului. Utilizatorul va fi singura persoană responsabilă de eventualele distrugeri cauzate calculatorului prin intermediul căruia este accesat Serviciul sau de alte pierderi de date ce pot rezulta din descărcarea oricăror materiale.

5. In cazul in care furnizorul depistează o acțiune ilegală sau care afectează buna funcționare a întregii rețele, işi rezerva dreptul de a deconecta fără o avertizare □n prealabil temporar sau definitiv clientul respectiv.

VII. Schimbarea acestei politici de securitate

~~Ne rezervam dreptul de a schimba acesta~~ Politica de securitate pote fi modificată în orice moment, de către serviciul IT, fără o notificare prealabilă a utilizatorilor, în condițiile aducerii la cunoştința Senatului Universității, în proxima şedință a acestuia, spre aprobare, a modificărilor survenite.

Referințe

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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 14.06.2012
Președinte: Prof.univ.dr. SORIN CURILĂ

10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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 Universității din Oradea

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

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

Politica de securitate a Universității 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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

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.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 27.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

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

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

   Aceste date vor fi copiate şi distribuite în cadrul Universității din Oradea doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

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

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

   Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii Universității.

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

6. Atribuții şi Responsabilități

Atribuțiile manageriale includ:

- Orice angajat sau compartiment al Universității 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 informațiilor.
- Administratorii de rețea / sistem / baze de date trebuie să asigure existența jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform regulamentelor sau procedurilor asociate.
- Administratorii de rețea / sistem / baze de date trebuie să asigure activarea tuturor mecanismelor de securitate.
- Administratorii de rețea / sistem / baze de date elaborează şi propune modificări ale politicii de securitate a sistemului RIC[1].
- Administratorii de rețea / 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 rețea / sistem / baze de date elaborează proceduri pentru identificarea utilizatorilor RIC[3]
- Administratorii de rețea / sistem / baze de date tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra RIC[4].
- Administratorii de rețea / sistem / baze de date facilitează evaluările legale, a cerințelor de tip "cele mai bune practici" pe măsură ce acestea devin recunoscute[5].

Atribuții ale utilizatorilor:

---

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

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

- 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.

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

- Utilizarea RIC se face numai în interes de serviciu.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

- Utilizatorii trebuie să anunțe Administratorii de rețea[6] în cazul în care se observă orice problemă / breșă în sistemul de securitate din cadrul Universității din Oradea cât și orice posibilă întrebuințare greșită sau încălcare a regulamentelor în vigoare.
- Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul RIC a Universității din Oradea.
- Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ 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 și/sau informații similare utilizate în scopuri de autorizare și 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 excepția cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universității din Oradea. Această listă va fi întocmită de către Departamente / centre și Facultăți, aprobată de către Serviciul Management Integrat IT și publicată de către Departamente / Centre și Facultăți.
- Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane; să degradeze performanțele sistemelor ce alcatuiesc RIC; să împiedice accesul unui utilizator autorizat la RIC; să obțină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente
- Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemelor ce alcatuiesc RIC. De exemplu, utilizatorii Universității din Oradea nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
- RIC ale Universității 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 Universității).
- Accesul la rețeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituției și Regulamentului pentru Utilizare Internet și Intranet.
- Angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale Universității.
- Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activitățile desfășurate prin intermediul sau folosind RIC din Universitatea din Oradea.
- Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Universității din Oradea folosind RIC.
- Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Universității din Oradea sau prejudicierea, indiferent de formă, a intereselor Universității.
- Fișierele electronice create, trimise, primite sau stocate pe Resurse Informatice proprii, închiriate, administrate sau în custodia și sub controlul Universității din Oradea, cad sub incidența reglementărilor legale privind proprietatea intelectuală și pot fi subiectul unor cereri de verificare / inspectare / accesare, conform legislației în vigoare

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

9. Măsuri Disciplinare

Încălcarea acestui regulament se sancționează 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 relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenților;
- Interzicerea accesului la Resursele Informatice şi de Comunicații.

Toate acțiunile care contravin legilor vor fi raportate organelor competente.

10. Alte Dispoziții

Acest Regulament are ca parte integrantă următoarele dispoziții:

1. Întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acțiunile 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 confidențialității datelor personale sau a accesului la informații folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversații telefonice, transmisie fax-uri şi alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronica poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare.
4. Departamentele/ centrele şi facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC.
5. Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială şi în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale şi în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar.
6. Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația şi datele trebuie protejate.
7. Departamentele / Centrele şi Facultățile trebuie să ofere facilitate corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor şi programelor împotriva întrebuințării greşite, în concordanță cu necesitățile 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 însoțit de Licență care să specifice clar drepturile de utilizare şi restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor si nu este permisă copierea ilegală a programelor comerciale. Serviciul Management Integrat IT, direct sau prin intermediul Departamentelor / Centrelor şi Facultăților, îşi rezervă dreptul de a şterge orice produs fără Licență de pe orice sistem din cadrul RIC.
9. Inginerii de sistem/Administratorii de rețea, direct sau prin intermediul Departamentelor / Centrelor şi Facultăților, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

11. Dispoziții Finale

1. Politica de Securitate a Universității 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 toți utilizatorii.
2. Serviciul Management Integrat IT are obligația 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 studenții şi contractele cu terți[7] care implică accesul la resursele sistemului Informatic şi de Comunicații al Universității, 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 Universității din Oradea.
5. Prezentul document şi componentele Planului de Securitate vor conține informații 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 Universității 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 Universității din Oradea.
7. Modificarea prevederilor unui Regulament / Procedură se face cu aprobarea conducerii Universității din Oradea. Fiecare modificare a conținutului va conduce la modificarea versiunii documentului şi a informațiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.
8. Planul de securitate va conține o listă a tuturor regulamentelor şi procedurilor aplicabile în sistemul RIC.

12.Referințe

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. http://www.iso17799software.com/what.htm
8. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul telecomunicațiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

[7] Trebuie să se procedeze in acest sens

APROBAT ÎN ŞEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 12.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

ROMÂNIA
MINISTERUL EDUCAȚIEI 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

Plan de Securitate
Utilizarea Resurselor Informatice si de Securitate
Universității din Oradea

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

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 27.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ

Plan de Securitate
Utilizarea Resurselor Informatice si de Securitate
Universității din Oradea

1. Introducere

Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii (abreviate RIC) sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Universitatea din Oradea.

Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii Universităţii şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

2. Scop

În acord cu legislaţia în vigoare în România, Regulamentele de ordine interioară ale Universităţii din Oradea, RIC sunt valori ale Universităţii din Oradea, care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român. Scopul acestor regulamente este acela de a asigura:

1. Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional şi a cercetării ştiinţifice;
2. Protejarea imaginii Universităţii din Oradea;
3. Protejarea investiţiilor Universităţii din Oradea pentru dezvoltarea sistemului informatic şi de comunicaţii propriu;
4. Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind RIC ale utilizatorilor autorizaţi: cadre didactice, personal administrativ, studenţi, colaboratori etc.
5. Educarea utilizatorilor RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
6. Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea RIC.

3. Audienţă

Regulamentele de utilizare a RIC ale Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

4. Proceduri de elaborare, modificare şi aprobare a Regulamentelor

1. Regulamentele de utilizare a RIC ale Universităţii din Oradea se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare Regulament să poată fi folosit cvasi-independent de celelalte.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

2. Regulamentele vor fi elaborate de către Serviciul Management Integrat IT (SMIIT) şi vor fi propuse pentru aprobare conducerii Universităţii din Oradea.
3. În contractele de muncă, contractele de şcolarizare cu studenţii şi contractele cu terţi[1] 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. Fiecare Regulament va conţine informaţii de identificare proprii şi se va specifica data la care acesta a fost aprobat şi data de la care acesta este aplicabil.
5. Regulamentele de utilizare a sistemului RIC vor fi disponibile în format electronic pe sit-ul web al Universităţii din Oradea - 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.
6. Modificarea prevederilor unui Regulament se face cu aprobarea conducerii Universităţii din Oradea. Fiecare modificare va include modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune este aplicabilă.
7. Prezentul document va conţine o listă a tuturor regulamentelor aplicabile în sistemul RIC.

[1] Trebuie să se procedeze in acest sens

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

5. Proceduri şi Regulamente Specifice

1. REGULAMENT de utilizare a Resurselor Informatice şi de Comunicaţii (Anexa 1)
2. REGULAMENT privind Confidenţialitatea Serviciilor Informatice şi de Comunicaţii (Anexa 2)
3. REGULAMENT de Acces la Reţeaua de Comunicaţii (Anexa 3)
4. REGULAMENT de Acces Administrativ (Anexa 4)
5. REGULAMENT privind accesul fizic la Resursele Informatice şi de Comunicaţii (Anexa 5)
6. REGULAMENT de tratare a incidentelor de securitate (Anexa 6)
7. REGULAMENT de monitorizare a Resurselor Informatice şi de Comunicaţii (Anexa 7)
8. REGULAMENT pentru Detectarea Accesului Neautorizat (Anexa 8)
9. REGULAMENT privind crearea şi utilizarea copiilor de siguranţă (backup) (Anexa 9)
10. REGULAMENT de Securizare a Serverelor (Anexa 10)
11. Regulament de Utilizare a reţelei Internet şi Intranet (Anexa 11)
12. REGULAMENT privind Configurarea Sistemelor Informatice pentru Acces la Reţeaua de Comunicaţii (Anexa 12)
13. REGULAMENT privind parolele de acces (Anexa 13)
14. REGULAMENT de administrare a conturilor de email (Anexa 14)
15. REGULAMENT privind sistemul de mesagerie electronica (Anexa 15)
16. REGULAMENT privind detectarea viruşilor (Anexa 16)
17. PROCEDURĂ PENTRU ALOCAREA UNEI ADRESE DE EMAIL (Anexa 21)

6. Referinţe

1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.dict.uvt.ro/regulamente/
4. 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. http://www.iso17799software.com/what.htm
8. 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.
9. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
10. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.

APROBAT ÎN ŞEDINŢA DE SENAT DIN
DATA DE 17.06.2013
Preşedinte: Prof.univ.dr. SORIN CURILĂ

14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
15. 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.
16. 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.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

APROBAT ÎN ȘEDINȚA DE SENAT DIN
DATA DE 17.06.2013
Președinte: Prof.univ.dr. SORIN CURILĂ