ROMÂNIA
MINISTERUL EDUCAŢIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal Oradea 1,Str. Universităţii nr. 1, Oradea, România
Telef: +40 0259 / 432830 +40 0259 / 408 190, Fax: +40 0259/ 432789
E-mail: rectorat@uoradea.ro, Pagina web: www.uoradea.ro

Politica de securitate a Campusului Universităţii din Oradea

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

Politica de securitate a Campusului Universităţii din Oradea

Condiţiile în care Universitatea din Oradea (abreviată UO) furnizează serviciul de acces la reţeaua 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 dispoziţie un hub central;

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

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

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

2. Utilizatorul are obligaţia de a pune la dispoziţia 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 conţin viruşi sau orice alt tip de cod, fişiere, sau programe care sunt create să distrugă, întrerupă sau să limiteze funcţionarea oricărui alt software, componente hardware sau echipament de telecomunicaţii;

4. Utilizatorul nu are dreptul:

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

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 reţele conectate sau nu la Internet, prin metode wired, wireless sau in alte tehnologii 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 obţinerea de foloase necuvenite prin exploatarea vulnerabilităţilor 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 obţine informaţii / rapoarte de la alte calculatoare utilizate pentru scopuri ilegale, cum ar fi *spamming* sau alte acţiuni ilegale.

III. Responsabilitatea pentru conţinutul documentelor.

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

Pentru toate informaţiile, 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 Reţele

UO nu este responsabil pentru situaţiile 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 reţelei.

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

1. încercarea de a proba, scana sau testa vulnerabilitatea unui sistem sau a unei reţele 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 reţea inclusiv, dar fără a se limita la, mijloace de supraîncărcare, "*flooding*" sau "*crashing*";

3. contrafacerea oricărui "header" TCP/IP sau a oricărei părţi din informaţia cuprinsă în acesta. Pentru protejarea reţelei, a resurselor furnizorului Internet, precum şi a celorlalţi clienţi, în cazul unor atacuri de tip "*Denial-of-Service*" având ca ţintă adrese Internet alocate

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

VI. Limitarea răspunderii

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

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

2. Exceptând dispoziţiile contrare din Contract, UO nu îşi asumă nicio responsabilitate privind orice fel de pagubă de orice natură provocată de Utilizator prin intermediul sau cu ajutorul IP-ului obţinut in momentul conectării. UO nu este responsabil de nici-un fel de daune directe, indirecte, accidentale sau pentru comunicaţii 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 terţă 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 informaţiilor care tranzitează Internetul;

3. Utilizatorul este de acord să exonereze de răspundere şi să despăgubească UO atât cu privire la orice pretenţie ridicata de către un terţ, rezultată din Utilizarea Serviciului sau a reţelei de comunicaţii a UO şi a Internetului de către Utilizator, cât şi cu privire la orice pierdere (directă, indirectă, pe cale de consecinţă sau de alta natură), costuri, acţiuni, procese, pretenţii, 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 obţinut în alt fel prin utilizarea Serviciului se află astfel la discreţia 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 acţiune ilegală sau care afectează buna funcţionare a întregii reţele, işi rezerva dreptul de a deconecta fără o avertizare în prealabil temporar sau definitiv clientul respectiv.

VII. Schimbarea acestei politici de securitate

Politica de securitate pote fi modificată în orice moment, de către serviciul IT, fără o notificare prealabilă a utilizatorilor, în condiţiile aducerii la cunoştinţa Senatului Universităţii, în proxima şedinţă a acestuia, spre aprobare, a modificărilor survenite.

Referinţe

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. 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.
18. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.