**ROMÂNIA**
**MINISTERUL EDUCAŢIEI NAȚIONALE**
**UNIVERSITATEA DIN ORADEA**

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

# REGULAMENT

## de tratare a incidentelor de securitate

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

# REGULAMENT de 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

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

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.
- *Echipă de Răspuns la Incidentele de Securitate a RIC* (ERIS): personalul responsabil de acţiunile 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 aplicaţie 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 reţelei. Prima utilizare a termenului descria un program care s-a multiplicat 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 datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă 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 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 integrităţii şi/sau confidenţialităţii informaţiei 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 informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

## REGULAMENT de tratare a incidentelor de securitate

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

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

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

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

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

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

7. Serviciul Management Integrat IT trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor 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 activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

10. În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare Serviciul Management Integrat IT va recomanda sancţiuni 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 acţiona ca ofiţer de legătură cu acestea.

## Măsuri Disciplinare

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

- In cazul angajatilor UO, se va proceda la suspendarea accesului la resurse, respectiv la alte masuri disciplinare – conform legislatiei in vigoare
- Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenţilor;
- Interzicerea accesului la Resursele Informatice şi de Comunicaţii.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

# Referinţe


1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.usamvcluj.ro/CIC/documente/Plan%20de%20securitate.pdf
4. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
5. ISO 17799 – Standard detaliat de securitate:
6. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.
7. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
8. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
9. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
10. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
11. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
12. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
13. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
14. 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.
15. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
16. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.