

# Politica de securitate a Universității de Vest din Timișoara

v.1.1.0 - [09-dec-2004]

## 1. Introducere

În acord cu prevederile din prezentul document, Resursele Informatice și de Comunicații (Resursele Informatice și de Comunicații) puse la dispoziție și administrate de Centrul de Comunicații și Informatizare (CCI) sunt bunuri strategice ale Universității de Vest din Timișoara care trebuie administrate ca resurse ale statului român.

Compromiterea securității acestor resurse poate afecta capacitatea Universității de Vest din Timișoara de a oferi servicii informatice și de comunicații, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilității instituției în fața partenerilor săi.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice,
- Să stabilească practici prudente și acceptabile privind utilizarea Resurselor Informatice și de Comunicații ale Universității de Vest din Timișoara,
- Să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice și de Comunicații privind responsabilitățile asociate unei astfel de utilizări.

## 2. Audiență

Politica de securitate a Resurselor Informatice și de Comunicații ale Universității de Vest din Timișoara se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a instituției.

Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile Politicii:

- Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- Colaboratorii Universității de Vest din Timișoara care au acces la Resursele Informatice și de Comunicații;
- Furnizorii Universității de Vest din Timișoara care au acces la Resursele Informatice și de Comunicații;
- Studenții Universității de Vest din Timișoara;

- Alte persoane, entități sau organizații care au acces la Resursele Informatice și de Comunicații.

### **3. Scop**

Politica de securitate a Resurselor Informatice și de Comunicații are ca scop asigurarea integrității, confidențialității și disponibilității informației.

*Confidențialitatea* se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul Universității de Vest din Timișoara, sunt proprietatea Universității în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la Resursele Informatice și de Comunicații.

*Integritatea* se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

*Disponibilitatea* se asigură prin funcționarea continuă a tuturor componentelor Resurselor Informatice și de Comunicații. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a Resurselor Informatice și de Comunicații.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii Resurselor Informatice și de Comunicații.

### **4. 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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (notebook-uri, 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.

*Centrul de Comunicații și Informatizare*: Responsabil la nivelul instituției cu administrarea Resurselor Informatice și de Comunicații Universității de Vest din Timișoara. Desemnarea Centrului de Comunicații și Informatizare are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea și aprobarea regulamentelor privind activitățile de administrare și utilizare a Resurselor Informatice și de Comunicații.

*Utilizator*: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Universitatea de Vest din Timișoara, 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 de Vest din Timișoara și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înlăptuirea de către utilizator a acțiunii respective.

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

## **5. Clasificarea Informațiilor**

Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât și pentru a determina pierderile potențiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:

- Publice
- Secrete
- Strict Secrete

Centrul de Comunicații și Informatizare și conducerea Facultăților/Departamentelor răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile din Universitatea de Vest din Timișoara trebuie să se regăsească în una din următoarele categorii:

*Publice:* Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul Universității de Vest din Timișoara. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituției sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Universității de Vest din Timișoara.

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

*Secrete:* În această categorie se includ informațiile care datorită valorii economice nu trebuie făcute publice. Se includ aici și informațiile pe care Universitatea de Vest din Timișoara 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 și distribuite în cadrul Universității de Vest din Timișoara doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

*Exemple:* clauze contractuale, conturi și parole folosite pe serverele de contabilitate sau gestiune a școlarității.

*Strict Secrete sau Confidențiale:* În această categorie se includ 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 șterse fără acordul scris al conducerii Universității.

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

## **6. Atribuții și Responsabilități**

*Atribuțiile manageriale includ:*

- Orice angajat sau compartiment al Universității de Vest din Timișoara trebuie să se asigure că managementul respectă prevederile prezentei Politici și a regulamentelor sau procedurilor asociate.
- Administratorii de rețea/sistem/baze de date trebuie să asigure existența jurnalelor și 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.
- Compartimentul de audit intern este responsabil de evaluarea schemei de clasificare a informațiilor.

*Atribuțiile Centrului de Comunicații și Informatizare includ:*

- Elaborează și propune modificări ale politicii de securitate a sistemului RIC.
- Elaborează și propune pentru aprobare regulamentele și procedurile de securitate a Resurselor Informatice și de Comunicații în conformitate cu politica de securitate a acestora.
- Elaborează proceduri pentru identificarea utilizatorilor Resurselor Informatice și de Comunicații.
- Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra Resurselor Informatice și de Comunicații.
- Facilitarea evaluărilor legale, a cerințelor de tip "cele mai bune practici" pe măsură ce acestea devin recunoscute.

*Atribuții ale utilizatorilor:*

- Să cunoască și să respecte prevederile Politicii de Securitate a Resurselor Informatice și de Comunicații.
- Să cunoască și să respecte prevederile tuturor Regulamentelor și/sau Procedurilor privind securitatea Resurselor Informatice și de Comunicații.
- Să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate direct sau indirect.

*Alte atribuții:*

- Toți partenerii Universității de Vest din Timișoara (furnizori, agenți, colaboratori etc.) trebuie să accepte și să respecte prezentul document și regulamentele specifice privind Resursele Informatice și de Comunicații.

## **7. Confidențialitate**

1. Fișierele electronice create, trimise, primite sau stocate folosind Resursele Informatice și de Comunicații administrate sau în custodia și sub controlul Universității de Vest din Timișoara nu au caracter personal și pot fi accesate oricând de către angajații autorizați din cadrul Centrului de Comunicații și Informatizare, Departamente și Facultăți fără înștiințarea utilizatorului conform Planului de Securitate.

2. În scopul administrării Resurselor Informatice și de Comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele Resurselor Informatice și de Comunicații în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității 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 Universității de Vest din Timișoara, orice incident de posibilă întrebuințare greșită sau încălcare a acestui regulament (prin contactarea Centrului de Comunicații și Informatizare).

4. Un mare număr de utilizatori (inclusiv studenți), pot accesa informații din exteriorul sistemului de comunicații al Universității de Vest din Timișoara. În aceste condiții este obligatorie păstrarea confidențialității informațiilor transmise din exteriorul Universității de Vest din Timișoara și a informațiilor obținute din interiorul instituției.

5. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele U\_UVTului pentru care nu au autorizație sau consimțământ explicit.

6. Nici un utilizator al Resurselor Informatice și de Comunicații Universității de Vest din Timișoara nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun Resursele Informatice și de Comunicații. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Universitatea de Vest din Timișoara.

7. 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 confidențiale ale Universității de Vest din Timișoara se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

## **8. Reguli de Utilizare Acceptabilă a Resurselor Informatice și de Comunicații**

- Utilizarea Resurselor Informatice și de Comunicații se face numai în interes de serviciu.

- Utilizatorii trebuie să anunțe CCIul în cazul în care se observă orice problemă/breșă în sistemul de securitate din cadrul Universității de Vest din Timișoara 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 Resurselor Informatice și de Comunicații Universității de Vest din Timișoara.

- Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din Resursele Informatice și de Comunicații pentru care nu au autorizație sau consimțământ explicit.

- Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup prin modem.

- 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 dispozitive 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 și a dreptului de autor (copyright).

- Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea Centrului de Comunicații și Informatizare, cu excepția cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universității de Vest din Timișoara. Această listă va fi întocmită de către Departamente și Facultăți, aprobată de către Centrul de Comunicații și Informatizare și publicată de către Departamente 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 Resursele Informatice și de Comunicații; să împiedice accesul unui utilizator autorizat la Resursele Informatice și de Comunicații; 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 Resursele Informatice și de Comunicații. De exemplu, utilizatorii Universității de Vest din Timișoara nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.

- Resursele Informatice și de Comunicații Universității de Vest din Timișoara nu trebuie folosite pentru beneficiul personal.

- Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Universitatea de Vest din Timișoara 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 Resursele Informatice și de Comunicații se supune aceluiași 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 Resursele Informatice și de Comunicații ale Universității.

- Utilizatorii care au acces la Resursele Informatice și de Comunicații Universității de Vest din Timișoara au obligația de a purta acte și sau legitimații care să ateste calitatea de utilizator autorizat în spațiile instituției.

- Utilizatorii vor folosi, exclusiv, numele de domeniu în toate activitățile desfășurate prin intermediul sau folosind Resursele Informatice și de Comunicații Universității de Vest din Timișoara.

- Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Universității de Vest din Timișoara folosind Resursele Informatice și de Comunicații.

- Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Universității de Vest din Timișoara sau prejudicierea, indiferent de formă, a intereselor Universității.

- Toate mesajele, fișierele și documentele - incluzând mesajele personale, fișierele și documentele - localizate în cadrul Resurselor Informatice și de Comunicații sunt proprietatea Universității și pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

## **9. Măsuri Disciplinare**

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

- Rezilierea contractului de muncă în cazul angajaților;
  - Încetarea relațiilor contractuale (de colaborare) în cazul contractanților, consultanților sau voluntarilor;
  - Suspendarea sau exmatricularea în cazul studenților;
  - Interzicerea accesului la Resursele Informatice și de Comunicații.
- Toate acțiunile care contravin legilor vor fi raportate organelor competente.

## **10. Alte Dispoziții**

- Acest Regulament are ca parte integrantă următoarele dispoziții:
- Întreg personalul este responsabil privind modul de utilizare a Resurselor Informatice și de Comunicații; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea Resurselor Informatice și de Comunicații.
  - Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament.
  - 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 și alte instrumente de conversație electronică. Utilizarea acestor instrumente de comunicație electronică poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare.
  - Departamentele și facultățile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a Resurselor Informatice și de Comunicații.
  - Orice informație folosită în sistemul RIC trebuie să fie păstrată confidențială și în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidențiale și în siguranță, tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar.
  - Toate programele de calculator, aplicațiile, codul sursă, codul obiect, documentația și datele trebuie protejate fiind proprietatea Universității.
  - Departamentele și Facultățile trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării Resurselor Informatice și de Comunicații, protejării datelor și programelor împotriva întrebuițării greșite, în concordanță cu necesitățile stabilite de acestea. Accesul trebuie să fie documentat, autorizat și controlat în mod corespunzător.
  - Orice program comercial utilizat în cadrul Resurselor Informatice și de Comunicații trebuie să fie însoțit de Licență care să specifice clar drepturile de utilizare și restricțiile produsului. Personalul trebuie să respecte prevederile Licențelor și nu este permisă copierea ilegală a programelor comerciale. Centrul de Comunicații și Informatizare, direct sau prin intermediul Departamentelor și Facultăților, își rezervă dreptul de a șterge orice produs fără Licență de pe orice sistem din cadrul Resurselor Informatice și de Comunicații.
  - \_CCIul, direct sau prin intermediul Departamentelor și Facultăților, își rezervă dreptul de a șterge, de pe orice sistem, orice program sau fișier care nu are legătură cu scopul muncii respective.

## 11. Dispoziții Finale

- Politica de Securitate a Universității de Vest din Timișoara impune dezvoltarea, gestionarea și punerea în practică de proceduri și/sau regulamente specifice. Toate procedurile și/sau regulamentele de securitate a Resurselor Informatice și de Comunicații fac parte din Planul de Securitate și sunt obligatorii pentru toți utilizatorii.

- Centrul de Comunicații și Informatizare are obligația de a revizui periodic prezenta Politică de Securitate și a propune dezvoltarea, modificarea Planului de Securitate.

- Prevederile Politicii de Securitate vor fi incluse în contractul de muncă, contractul de școlarizare cu studenții și toate contractele cu terți (dacă activitatea acestora are legătură cu sistemul Informatic și de Comunicații al Universității).

- Componentele Planului de Securitate vor fi elaborate de către Centrul de Comunicații și Informatizare și vor fi propuse pentru aprobare conducerii Universității de Vest din Timișoara.

- Prezentul document și componentele Planului de Securitate vor conține informații de identificare proprii și se va specifica data la care acestea au fost aprobate și data de la care intră în vigoare.

- Prezentul document și Planul de Securitate a sistemului Resurselor Informatice și de Comunicații vor fi disponibile în format electronic pe sit-ul web al Universității de Vest din Timișoara și pe sit-ul web al Centrului de Comunicații și Informatizare. Se recomandă ca aceste documente să fie disponibile sau să se facă trimitere la acestea de pe toate sit-urile web din cadrul Universității de Vest din Timișoara.

- Modificarea prevederilor unui Regulament/Procedură se face cu aprobarea conducerii Universității de Vest din Timișoara. Fiecare modificare a conținutului va conduce la modificarea versiunii documentului și a informațiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.

- Planul de securitate va conține o listă a tuturor regulamentelor și procedurilor aplicabile în sistemul Resurselor Informatice și de Comunicații.

## 12. Referințe

Politica de securitate a UAIC -

<http://www.dcd.uaic.ro/default.php?t=site&pgid=138>

RFC 1244 - Site Security Handbook: <http://www.ietf.org/rfc/rfc1244.txt>

ISO 17799 - Standard detaliat de securitate:

<http://www.iso17799software.com/what.htm>

Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor.

Lege nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.

Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.

HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.



Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

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.

Hotărâre nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.

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

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.