



Documente de referință:

Carta Universității de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș **UMFST-REG-01**

Codul de etică și deontologie profesională **UMFST-REG-02**

Regulamentul de organizare și funcționare (ROF) a UMFST Târgu Mureș **UMFST-REG-10**

RFC 2196 – Site Security Handbook: <https://tools.ietf.org/html/rfc2196>

ISO/IEC 27002:2013 – Cod de bună practică pentru managementul securității informației:

<http://www.iso27001security.com/html/27002.html>

Legea nr. 235/2015 - modificarea Legii nr. 506/2004 - prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

Legea nr. 1/2011 - Legea educației naționale.

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.

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.

Legea 213/2002 (IT) - privind aprobarea Ordonanței Guvernului nr. 124/2000 pentru completarea cadrului juridic privind dreptul de autor și drepturile conexe prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio și video, precum și a programelor pentru calculator;

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

REGULAMENTUL POLITICII DE SECURITATE IT la UMFST G.E.PALADE TG. MUREȘ

*Regulation of the policy for security IT within George Emil Palade U.M.P.H.T.
Târgu Mures*

Cod regulament: UMFST-REG-68

Ediția 02

Întocmit: Rizoli Iulian Dănuț

Data: 28. ianuarie 2019

Verificat: Consiliul de Administrație

Data: 11. februarie 2019

Aprobat: Senat

Data: 20. martie 2019

Data intrării în vigoare:	21 martie 2019
Data retragerii:	



Capitolul I. Dispoziții generale

Art.1. Documentele interne de reglementare a utilizării Resurselor Informatice și de Comunicații sunt elaborate pentru a stabili un cadru corect, legal și eficient de utilizare a tehnologiei informației și comunicațiilor în Universitatea de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș.

Art.2. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acestea vizează protejarea imaginii Universității și a investițiilor acesteia pentru dezvoltarea sistemului informatic și de comunicații.

Art.3. Rețeaua informatică a UMFST G.E. Palade Tg. Mureș sprijină procesul de învățământ și de cercetare prin mijloacele de comunicare și serviciile specifice oferite de rețelele de calculatoare conectate la Internet.

Capitolul II. Politica de securitate

Art.4. Compromiterea securității resurselor IT poate afecta capacitatea Universității de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș 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 IT
- Să instruiască utilizatorii care au dreptul de folosire a resurselor IT privind responsabilitățile asociate unei astfel de utilizări.

Art.5. Clasificarea informațiilor din punct de vedere al securității și integrității informațiilor:

a) Informații Publice

Acestea sunt informații accesibile oricărui utilizator din interiorul sau exteriorul Universității. Exemplu de astfel de date sunt cele de la avizier, pe site-urile Web, sau informațiile de presă. Persoanele care fac publice aceste date sunt special denumite de către Conducerea Universității și poartă responsabilitatea publicării acestor date.

b) Informații Secrete

Aceste informații includ date care dacă sunt făcute publice aduc daune economice sau de imagine Universității. Astfel de date pot fi: clauze contractuale, informații obținute prin



participare la licitații, conturi sau parole etc. Aceste date trebuie protejate prin clauze de confidențialitate.

c) Informații Strict Secrete

În această categorie intră date ce nu pot fi copiate, distribuite sau șterse fără acordul scris al Conducerii Universității și care ar aduce mari prejudicii în caz de compromitere. Ex: parole la servere importante, date examene de admitere, rezidențiat, chei de criptare etc.

II. 1. Audiență

Art.6. Politica de securitate a resurselor IT în Universitatea de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a instituției.

Art.7. Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile Politicii:

- a) Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- b) Colaboratorii Universității care au acces la resursele IT;
- c) Furnizorii Universității care au acces la resursele IT;
- d) Studenții Universității;
- e) Alte persoane, entități sau organizații care au acces la resursele IT.

II. 2. Definiții

Art.8. *Resurse IT:* 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), 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.



Art.9. *Inginerul de sistem/Administratorul de rețea este și Administratorul Resurselor Informatică si de Comunicare:* Responsabil la nivelul instituției cu administrarea Resurselor IT din cadrul Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș.

Art.10. *Utilizator:* O persoană, o aplicație automatizată sau process utilizator autorizat de către, în conformitate cu procedurile și regulamentele în vigoare, să folosească Resursele IT.

Art.11. *Abuz de privilegii:* Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Universității de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș 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.

Art.12. *Furnizor:* Persoană fizică/juridică care oferă bunuri sau servicii Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș în baza unui contract comercial sau de colaborare.

II. 3. Atribuții si obligații

Art.13. Administratorii rețelei, reprezentați prin Serviciul Rețele de Calculatoare, Comunicații și Informatizare (RCCI), au următoarele atribuții cu privire la Politicile de Securitate:

- a) Elaborează și propune modificări ale Politicii de Securitate;
- b) Elaborează și propune pentru aprobare regulamentele și procedurile de securitate;
- c) Tratarea incidentelor de securitate;
- d) Elaborează proceduri pentru identificarea utilizatorilor.

Art.14. Atribuțiile utilizatorilor sunt:

- a) Să cunoască și să respecte prevederile Politicii de Securitate
- b) Să cunoască și să respecte prevederile regulamentelor și procedurilor de securitate
- c) Să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate direct sau indirect.

Art.15. Toți partenerii Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș trebuie să accepte și să respecte aceste politici de securitate.

II.4. Confidențialitatea Informațiilor

Art.16. Fiecare utilizator este responsabil în mod direct de modul de utilizare a resurselor Universității.

Art.17. Nu există nici o asigurare a confidențialității datelor personale sau a accesului la informații, mesagerie electronică, navigare Web, conversații telefonice, acces la rețelele Wireless,



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.

Art.18. Modul de acces la resursele Universității trebuie reglementat și monitorizat împotriva întrebuintării greșite sau rău voite.

Art.19. Orice sistem din proprietatea Universității trebuie să fie însoțit de Fișa Sistemului de Calcul care conține licențele și aplicațiile ce pot fi folosite.

Art.20. Serviciul RCCI își rezervă dreptul de a șterge, de pe orice sistem orice program sau fișier ce nu are legătura cu scopul muncii respective, sau contravine politicilor Universității. De asemenea se poate suspenda functionarea oricărui echipament care poate afecta funcționarea sistemelor din cadrul Universității.

Art.21. Personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele Universității 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).

Art.22. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș, orice incident de posibilă întrebuintare greșită sau încălcare a acestui regulament.

Art.23. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universității de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș pentru care nu au autorizație sau consimțământ explicit.

Art.24. Nici un utilizator al sistemelor din Universitatea de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Universitatea de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș.

Capitolul III. Planul de securitate

Art.25. Planul de securitate conține toate regulile și procedurile aplicabile în sistemul Resurselor Informatice și de Comunicații ale Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș.



Art.26. Planul de securitate are ca scop principal protejarea utilizatorilor și colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea, acesta are ca scop protejarea imaginii Universității și a investițiilor acesteia pentru dezvoltarea sistemului informatic și de comunicații, protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate cu ajutorul Resurselor Informatică și de Comunicații ale utilizatorilor autorizați: cadre didactice, personal administrativ, studenți, colaboratori etc.

Art.27. Regulile au fost elaborate pentru fiecare activitate specifică domeniului și au fost concepute în așa fel încât fiecare să poată fi folosită cvasi independent de celelalte.

Art.28. Regulile și procedurile din planul de securitate au rolul:

- a) de a fi corecte, echitabile și eficiente pentru folosirea resurselor informatice și de comunicație în vederea sprijinirii procesului didactic și al cercetării științifice.
- b) de a educa utilizatorii resurselor informatice și de comunicație în ceea ce privește responsabilitățile asociate cu utilizarea acestora.
- c) de a fi compatibile cu regulamentele, statutul și atribuțiile stabilite pentru administrarea resurselor informatice și de comunicații.

Art.29. Regulile de utilizare a Resurselor Informatică și de Comunicații a Universității de de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade" din Târgu Mureș se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la aceste resurse.

III. 1. Procedee și reglementări

Reglementări privind accesul la resursele informatice ale UMFST G.E. Palade Tg. Mureș

Art. 30. Regulamentul privind accesul la rețeaua intranet/internet și utilizarea aplicațiilor **software** parte integrantă din Regulamentul de organizare și funcționare (ROF) a UMFST G.E. Palade Tg. Mureș, prevede următoarele **reguli privind accesul la email**:

- a) Orice parolă trebuie să fie **complexă**. Pentru parole se respectă **Regulile privind parolele de acces** de mai jos Informaticianul, cu drepturi de administrator pe serverul de email, creează contul de email cu o parola inițială, care va fi schimbată de utilizator la prima accesare a contului.
- b) Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces și datele din acestea.
- c) Utilizatorii nu trebuie să trimită, retrimite sau să primească informații confidențiale sau sensibile ce privesc "Universitatea de Medicină, Farmacie, Științe și Tehnologie "George Emil Palade"



din Târgu Mureș”, folosind conturi utilizator care nu sunt proprietatea Universității. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum și adrese de email puse la dispoziție de alți Furnizorii de Servicii Internet.

Art. 31. De asemenea potrivit Regulamentului privind accesul la rețeaua intranet/internet și utilizarea aplicațiilor software parte integrantă din Regulamentul de organizare și funcționare (ROF) a UMFST G.E. Palade Tg. Mureș, referitor la **accesul la email, este interzis:**

- a) Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
- b) Folosirea sistemului de mesagerie electronică în scopuri personale;
- c) Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- d) Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- e) Folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
- f) Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deserveșc instituția.

Art. 32. Regulamentul privind accesul la rețeaua intranet/internet și utilizarea aplicațiilor software parte integrantă din Regulamentul de organizare și funcționare (ROF) a UMFST G.E. Palade Tg. Mureș, prevede următoarele **reguli privind accesul la email:** - Serviciul RCCI asigură confidențialitatea datelor personale sau a accesului la informații folosind poșta electronică sau alte instrumente de conversație electronică în limitele competențelor, a posibilităților tehnice existente și a limitelor impuse de prevederile legale în vigoare.

III. 2. Reglementari privind securitatea datelor

Art. 33. Securizarea serverelor se realizează prin următoarele reguli:

- a) Serverele trebuie să fie într-o locație cu acces securizat; accesul este restricționat doar la personalul tehnic autorizat;
- b) Instalarea sistemului de operare dintr-o sursă aprobată;
- c) Setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare;
- d) Dezactivarea sau schimbarea parolelor conturilor predefinite;
- e) Crearea și utilizarea copiilor de siguranță (backup).

Art. 34. Regulile privind **parolele de acces** sunt următoarele:

- a) Orice parolă ar trebui să fie complexă și să aibă o lungime minimă de 8 caractere. O parolă



complexă este un șir de caractere compus din litere minuscule, majuscule, cifre și simboluri (%\$#&^* ...). Criterii pentru stabilirea unei parole:

- a. nu este deloc recomandată folosirea simplă a datelor personale (ex: data nașterii, nume, prenume etc.) ca parole
- b. folosiți cifre și simboluri ușor de asociat prin forma lor cu litere. De exemplu: a=@, B=8, E=3, i=1, l=!, O=0(zero), s=\$. Exemplu: Așa **nu** EX: popdorin1974; Așa **da** EX: #p0pd0r1n!974
- c. faceți asocieri după ceva ce vă place: o carte, titlul unei melodii, titlul unui film, personajele dintr-un film etc. și trasați-vă niște reguli de formare a parolei pe care să le folosiți de fiecare dată când aveți nevoie de o parolă nouă.
- b) Nu vă notați parolele pe hârtii.
- c) Nu folosiți aceeași parolă pentru mai multe conturi.
- d) 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 (ex. parolele mele.rar).
- e) Evitați să păstrați parole în agende electronice, telefoane mobile – pot fi furate.
- f) Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile.
- g) 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.
- h) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice.
- i) Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
- j) Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
- k) 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.
- l) 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.

Art. 35. Alte reglementări privind securitatea sunt cele care urmează, acestea se referă la activități **interzise** precum:

- a) Activități comerciale neautorizate;



- b) Trafic masiv de informații sau trafic de informații cu caracter frivol, obscen și pornografic;
- c) Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizați;
- d) Ștergerea sau alterarea datelor altor utilizatori;
- e) Tentativele de descoperire și de folosire a parolelor altor utilizatori;
- f) Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;
- g) Provocarea deliberată de defectiuni hardware și software;
- h) Perturbarea traficului rețelei Universității;
- i) Generarea de trafic neacademic;
- j) Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică, cărți, etc.);
- k) Generarea de spam;
- l) Flood (indiferent de natura acestuia), de exemplu: ping flood;
- m) Răspândirea de aplicații de tip virus, troieni, viermi, spyware sau altele;
- n) Folosirea de aplicații de tip key-logere;
- o) Modificarea adresei MAC a plăcii de rețea;
- p) Setările pentru IP și DNS, altfel decât cu "Obtain an IP/DNS address automatically" , fără autorizație din partea Serviciului RCCI;
- q) Utilizarea de programe pentru scanarea rețelei, exploit-uri;
- r) Realizarea de tunele;
- s) Transmiterea de mesaje cu caracter comercial;
- t) Publicitatea cu caracter comercial;
- u) Folosirea de software fără licență pe calculatoarele din universitate sau conectate la rețeaua universității.

III.3. Reglementări/procedee administrare informații

Art. 36. Regulile specifice privind administrarea informațiilor și activități de mentenanță sunt conținute în proceduri specifice elaborate de Serviciul Rețele de Calculatoare, Comunicații și Informatizare:

- *Procedură operațională Administrarea conținutului informațional al paginilor web*
- *Procedură operațională Administrarea adreselor de email instituționale*
- *Procedură operațională Depanare mentenanță sisteme de calcul*

Art. 37. Reguli de administrare a conturilor de email:



- a) Fiecare cont de email creat pe domeniul umfst.ro trebuie să aibă asociate o cerere și o aprobare corespunzătoare.
- b) Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces.
- c) Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
- d) Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu Regulile privind Parolele de Acces.
- e) Numărul de mesaje din Inbox este limitat la ~5000. În momentul în care se ajunge la această limită un script va muta mesajele din Inbox într-un folder cu data respectivă. Excepție de la această regulă fac persoanele care au funcții de conducere, precum și cele din secretariate.
- f) Pentru păstrarea tuturor mesajelor primite este necesară instalarea unui client local de email (ex: Mozilla Thunderbird, Outlook express etc.) pe calculatorul individual al fiecărui utilizator.
- g) Regula de la punctul e) nu se aplică pentru perioadele de vacanță. Orice altă situație particulară (izolată) trebuie precizată Serviciului RCCI.
- h) La cererea conducerii autorizate din Universitate, Serviciul RCCI trebuie să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

Senatul Universității de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureș a aprobat prezentul regulament în data de 20 martie 2019 și intră în vigoare la data de 21 martie 2019 .
