Documente de referinţă:

Carta Universității de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş ***UMFST-REG-01***
Codul de etică și deontologie profesională ***UMFST-REG-02***
Regulamentul de organizare și funcționare (ROF) a UMFST Târgu Mureş ***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 electroniceLege 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 educatiei nationale.
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.
Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
Legea 213/2002 (IT) - privind aprobarea Ordonanţei Guvernului nr. 124/2000 pentru completarea cadrului juridic privind dreptul de autor şi drepturile conexe prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio şi video, precum şi a programelor pentru calculator;
Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.

REGULAMENTUL POLITICII DE SECURITATE IT la U.M.F.S.T. TÂRGU-MUREŞ

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

Cod regulament: UMFST-REG-68

Ediţia 02

Întocmit: Rizoli Iulian Dănuț — Data: 28. ianuarie 2019

Verificat: Consiliul de Administraţie — 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 şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Universitatea de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş.

Art.2. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acestea vizează protejarea imaginii Universităţii şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

Art.3. Reţeaua informatică a UMFST Târgu-Mureș sprijină procesul de învăţământ şi de cercetare prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare conectate la Internet.

Capitolul II. Politica de securitate

Art.4. Compromiterea securităţii resurselor IT poate afecta capacitatea Universității de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş 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 resurselor IT
- Să instruiască utilizatorii care au dreptul de folosire a resurselor IT privind responsabilităţile asociate unei astfel de utilizări.

Art.5. Clasificarea informaţiilor din punct de vedere al securității şi integrității informaţiilor:

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 acestă categorie intră date ce nu pot fi copiate, distribuite sau șterse fără acordul scris al Conducerii Universității și care ar aduce mari prejudiii în caz de compromitere. Ex: parole la servere importane, 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 din Târgu Mureş se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.

Art.7. Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Politicii:

a) Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
b) Colaboratorii Universităţii care au acces la resursele IT;
c) Furnizorii Universităţii care au acces la resursele IT;
d) Studenţii Universităţii;
e) Alte persoane, entităţi sau organizaţii care au acces la resursele IT.

II. 2. Definiţii

Art.8. *Resurse IT*: 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.

Art.9. *Inginerul de sistem/Administratorul de reţea este şi Administratorul Resurselor Informatice si de Comunicare*: Responsabil la nivelul instituţiei cu administrarea Resurselor IT din cadrul Universității de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş.

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

Art.11. *Abuz de privilegii:* Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Universității de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş 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.

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

II. 3. Atribuții si obligații

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

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

Art.14. Atribuțiile utilizatorilor sunt:

a) Să cunoasca și să respecte prevederile Politicii de Securitate
b) Să cunoască și să respecte prevederile regulamentelor şi procedurilor de securitate
c) Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

Art.15. Toți partenerii Universității de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş 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 confidenţialităţii datelor personale sau a accesului la informaţii, mesagerie electronică, navigare Web, conversaţii telefonice, acces la rețelele Wireless, transmisie fax-uri şi alte instrumente de conversaţie electronică. Utilizarea acestor instrumente de comunicaţie electronică poate fi monitorizată în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.

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

Art.19. Orice sistem din proprietatea Universității trebuie sa fie însoțit de Fișa Sistemului de Calcul care conține licențele și aplicațiile ce pot fii 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 Universitătii. De asemena se poate suspenda functionarea oricărui echipament care poate afecta functioanarea sistemelor din cadrul Universității.

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

Art.22. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universităţii de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.

Art.23. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universităţii de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş pentru care nu au autorizaţie sau consimţământ explicit.

Art.24. Nici un utilizator al sistemelor din Universitatea de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Universitatea de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş.

Capitolul III. Planul de securitate

Art.25. Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale Universității de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş.

Art.26. Planul de securitate are ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acesta are ca scop protejarea imaginii Universităţii şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul Resurselor

Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: cadre didactice, personal administrativ, studenţi, colaboratori etc.

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

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

a) de a fi corecte, echitabile şi eficiente pentru folosirea resurselor informatice și de comunicație în vederea sprijinirii procesului didactic şi al cercetării ştiinţifice.
b) de a educa utilizatorii resurselor informatice și de comunicație în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.
c) de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Art.29. Regulile de utilizare a Resurselor Informatice şi de Comunicaţii a Universității de de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş 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 Tîrgu 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 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) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces și datele din acestea.
c) Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc *“Universitatea de Medicină, Farmacie, Științe și Tehnologie din Târgu Mureş”*, folosind conturi utilizator care nu sunt proprietatea Universităţii. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi 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 Tg. Mureș, referitor la **accesul la email**, **este interzis:**

a) Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
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 identităţi 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 deservesc instituţia.

Art. 32. Regulamentul privind accesul la rețeaua intranet/internet și utilizarea aplicațiilor software parte integrantă din Regulamentul de organizare și funcționare (ROF) a UMFST Tg. Mureș, prevede următoarele **reguli privind accesul la email:** - Serviciul RCCI asigură confidențialitatea datelor personale sau a accesului la informații folosind poşta electronică sau alte instrumente de conversaţie electronică in limitele competentelor, a posibilităţilor tehnice existente şi 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 protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
d) Dezactivarea sau schimbarea parolelor conturilor predefinite;
e) Crearea şi utilizarea copiilor de siguranţă (backup).

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

a) 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 (%$#&^* …). Criterii pentru stabilirea unei parole:
    a. nu este deloc recomandată folosirea simplă a datelor personale (ex: data naşterii,

nume, prenume etc.) ca parole

b. folosiţi cifre şi simboluri uşor de asociat prin forma lor cu litere. De exemplu: a=@, B=8, E=3, i=1, I=!, O=0(zero), s=$. Exemplu: Aşa **nu** EX: popdorin1974; Aşa **da** EX: #p0pd0r1n!974

c. faceţi asocieri dupa ceva ce vă place: o carte, titlul unei melodii, titlul unui film, personajele dintr-un film etc. şi trasaţi-vă nişte reguli de formare a parolei pe care să le folosiţi de fiecare dată când aveţi nevoie de o parolă nouă.

b) Nu vă notaţi parolele pe hârtii.

c) Nu folosiţi aceeaşi parolă pentru mai multe conturi.

d) Dacă aveţi multe parole le puteţi scrie într-un fişier, însă criptaţi acel fişier şi asiguraţi-vă că nu-l veţi pierde. Evitaţi denumirea acelui fişier cu una explicită (ex. parolelemele.rar).

e) Evitaţi să păstraţi parole în agende electronice, telefoane mobile – pot fi furate.

f) Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile.

g) Aveţi grijă la facilitatea browser-elor de reţinere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucraţi e folosit de mai multe persoane.

h) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor 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) Activităţi comerciale neautorizate;

b) Trafic masiv de informaţii sau trafic de informaţii cu caracter frivol, obscen şi pornografic;

c) Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizaţi;

d) Ştergerea sau alterarea datelor altor utilizatori;

e) Tentativele de descoperire şi 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 şi software;
h) Perturbarea traficului reţelei 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 aplicaţii de tip virus, troieni, viermi, spyware sau altele;
n) Folosirea de aplicaţii de tip key-logere;
o) Modificarea adresei MAC a plăcii de reţea;
p) Setările pentru IP şi DNS, altfel decât cu "Obtain an IP/DNS address automatically" , fără autorizație din partea Serviciului RCCI;
q) Utilizarea de programe pentru scanarea reţelei, exploit-uri;
r) Realizarea de tunele;
s) Transmiterea de mesaje cu caracter comercial;
t) Publicitatea cu caracter comercial;
u) Folosirea de software fără licenţă pe calculatoarele din universitate sau conectate la reteaua universității.

III.3. Reglementări/procedee administrare informații

Art. 36. Regulile specifice privind administrarea informaţiilor şi activităţi de mentenanţă sunt conţinute în proceduri specifice elaborate de Serviciul Reţele de Calculatoare, Comunicaţii şi Informatizare:

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

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

a) Fiecare cont de email creat pe domeniul umftgm.ro trebuie să aibă asociate o cerere şi o aprobare corespunzătoare.

b) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor 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 şi 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. Excepţie de la această regulă fac persoanele care au funcţii de conducere, precum şi 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 punctual e) nu se aplică pentru perioadele de vacanţă. Orice altă situaţie particulară (izolată) trebuie precizată Serviciului RCCI.

h) La cererea conducerii autorizate din Universitate, Serviciul RCCI trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

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