MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA „1 DECEMBRIE 1918" DIN ALBA IULIA
SENATUL UNIVERSITĂȚII

REGULAMENT DE UTILIZARE A REȚELEI DE CALCULATOARE DIN CADRUL UNIVERSITĂȚII „1 DECEMBRIE 1918" DIN ALBA IULIA

UNIVERSITATEA „1 DECEMBRIE 1918" DIN ALBA IULIA	**COD: R-SFDA-31**	**Ediția: 1**
	REGULAMENT DE UTILIZARE A REȚELEI DE CALCULATOARE DIN CADRUL UNIVERSITĂȚII „1 DECEMBRIE 1918" DIN ALBA IULIA	**Revizia: 0**
		Aprobat SENAT Data: 27.11.2019

	Nume și prenume	**Funcția**	**Data**	**Semnătura**
ELABORAT	Despa Otilia Violeta	Șef Birou IT	20.11.2019	
AVIZAT	Găban Vasile Lucian	Director General Administrativ	22.11.2019	
	Scheau Ioan	Președinte Comisia pentru învățământ, evaluarea calității, strategii, dezvoltare și promovare instituțională	27.11.2019	

INDICATORUL APROBĂRILOR ȘI AL REVIZIILOR

Nr. crt.	**Ediția**	**Revizia**	**Data aprobării în Senat**
1.	1	0	27.11.2019

1. Dispoziţii generale

În acord cu prevederile prezentului regulament, Resursele Informatice şi de Comunicaţii (RIC) sunt puse la dispozitie şi administrate de către Biroul IT al Universităţii "1 Decembrie 1918" din Alba Iulia.

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 cadrul Universităţii "1 Decembrie 1918" din Alba Iulia.

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 sistemului informatic şi de comunicaţii.

Reţeaua informatică a UAB sprijină procesul de învăţământ şi de cercetare prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare.

Compromiterea securităţii acestor resurse poate afecta capacitatea Universităţii de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau la distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii instituţiei în faţa partenerilor săi. Prin urmare, prezentul regulament este motivat tehnic de necesitatea menţinerii în funcţiune, în condiţii de securitate, a reţelei UAB, precum şi de necesitatea dezvoltării normale a unei resurse de informare.

Scopul urmărit de politica de securitate este acela de asigurare a integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi stabilirea cadrului necesar pentru elaborarea regulilor şi procedurilor de securitate.

1. Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul UAB sunt proprietatea Universităţii în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii.

2. Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

3. Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor Resurselor Informatice şi de Comunicaţii. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a Resurselor Informatice şi de Comunicaţii.

2. Documente de referinţă

Orice activitate care se desfăşoară prin intermediul reţelei UAB trebuie să respecte legislaţia în vigoare (internă şi internaţională):

- Legea nr. 8/1996, privind dreptul de autor şi drepturile conexe, modificată si completată prin Legea nr. 15 din 2019;
- HG 58/1998 – pentru aprobarea Strategiei naţionale de informatizare şi implementare în ritm accelerat a societăţii informaţionale şi a Programului de acţiuni privind utilizarea pe scară largă şi dezvoltarea sectorului tehnologiilor informaţiei în România;
- Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificarile si completarile ulterioare;

- Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date si Legea nr. 190 din 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);
- HG 1609/2008, privind organizarea şi funcţionarea Agenţiei ARNIEC/RoEduNet;
- Convenţia privind Criminalitatea Informatică a Consiliului Europei.

Legislaţia primară va fi actualizată cu modificările şi completările ulterioare, dar şi cu alte acte normative relevante în domeniul securităţii informatice.

3. Definiţii

Intranet - reţeaua internă de calculatoare.

Cont - o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul.

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: servere, staţii de lucru, laptop-uri, echipament de laborator conectat la reţea şi controlat prin calculator, 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 este şi Administratorul Resurselor Informatice si de Comunicare - persoana responsabilă la nivelul instituţiei cu administrarea Resurselor IT.

Utilizator - o persoană, o aplicaţie automatizată sau proces utilizator autorizat, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele IT.

Abuz de privilegii - orice acţiune întreprinsă în mod voit de către un utilizator, care vine în contradicţie cu regulamentele UAB 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 UAB în baza unui contract comercial sau de colaborare.

4. Politica de securitate

Politica de securitate este alcătuită 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

Informatice şi de Comunicaţii ale UAB şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.

Clasificarea informaţiilor din punct de vedere al securităţii şi integrităţii informaţiilor:

1. **Informaţii Publice** - acestea sunt informaţii accesibile oricărui utilizator din interiorul sau exteriorul Universităţii. Exemplu de astfel de date sunt cele de la avizier, pe site-urile Web, sau informaţiile de presă.

2. **Informaţii Secrete** - aceste informaţii includ date care dacă sunt făcute publice aduc daune economice sau de imagine Universităţii. Astfel de date pot fi: clauze contractuale, informaţii obţinute prin participare la licitaţii, conturi sau parole etc. Aceste date trebuie protejate prin clauze de confidenţialitate.

3. **Informaţii Strict Secrete** - în acestă categorie intră date ce nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii Universităţii şi care ar aduce mari prejudicii în caz de compromitere. Ex: parole de acces la servere importante, chei de criptare etc.

Politica de securitate a resurselor IT în Universitatea "1 Decembrie 1918" din Alba Iulia se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.

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

1. Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
2. Colaboratorii Universităţii care au acces la resursele IT;
3. Furnizorii Universităţii care au acces la resursele IT;
4. Studenţii Universităţii;
5. Alte persoane, entităţi sau organizaţii care au acces la resursele IT.

Administratorii reţelei, angajaţi în cadrul Biroului IT al Universităţii, au următoarele atribuţii cu privire la Politicile de Securitate:

- Elaborează şi propun modificări ale Politicii de Securitate;
- Elaborează şi propun pentru aprobare regulamentele şi procedurile de securitate;
- Tratarea incidentelor de securitate;
- Elaborează proceduri pentru identificarea utilizatorilor.

Atribuţiile utilizatorilor sunt:

1. Să cunoască şi să respecte prevederile Politicii de Securitate;
2. Să cunoască şi să respecte prevederile regulamentelor şi procedurilor de securitate;
3. Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

Toţi partenerii Universităţii "1 Decembrie 1918" din Alba Iulia trebuie să accepte şi să respecte aceste politici de securitate.

4.1. Confidenţialitatea informaţiilor

Fiecare utilizator este responsabil în mod direct de modul de utilizare a resurselor Universităţii.

Nu există nicio asigurare a confidenţialităţii datelor personale sau a accesului la informaţii, mesagerie electronică, navigare Web, conversaţii telefonice, acces la reţelele 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.

Modul de acces la resursele Universităţii trebuie reglementat şi monitorizat împotriva întrebuinţării greşite sau rău voite.

Orice sistem din proprietatea Universităţii trebuie sa fie însoţit de Fişa Sistemului de Calcul care conţine licenţele şi aplicaţiile ce pot fi folosite.

Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele sunt proprietatea Universităţii şi trebuie să fie protejate.

Biroul IT îşi rezervă dreptul de a şterge, de pe orice sistem orice program sau fişier ce nu are legătura cu scopul muncii respective, sau contravine politicilor Universităţii. De asemenea se poate suspenda funcţionarea oricărui echipament care poate afecta funcţionarea sistemelor din cadrul Universităţii.

Personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele Universităţii în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor.

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul UAB, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.

Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universităţii pentru care nu au autorizaţie sau consimţământ explicit.

Niciun utilizator al sistemelor din UAB 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.

Informaţiile publicate electronic de către UAB pe site-ul propriu www.uab.ro şi în subdomeniile acestuia sunt proprietate a Universităţii. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către UAB în beneficiul comunităţii publice, în scop de informare asupra programelor academice şi a activităţii UAB.

Orice utilizare a informaţiilor de pe site-urile publice ale UAB în domeniul **uab.ro** de către persoane particulare sau organizaţii în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora. În acest caz, UAB îşi rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.

Fişierele electronice create, trimise, primite sau stocate folosind Resursele Informatice şi de Comunicaţii administrate sau în custodia şi sub controlul Universităţii nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi din cadrul UAB, fără înştiinţarea utilizatorului.

5. Planul de securitate

Politica de securitate a Universităţii impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidenţialitatea şi disponibilitatea informaţiei în utilizarea RIC.

Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale UAB.

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.

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.

Regulile şi procedurile din planul de securitate au rolul:

1. de a fi corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţie în vederea sprijinirii procesului didactic şi al cercetării ştiinţifice;
2. de a educa utilizatorii resurselor informatice şi de comunicaţie în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
3. de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Regulile de utilizare a Resurselor Informatice şi de Comunicaţii ale UAB se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la aceste resurse.

5.1. Procedee şi reglementări

Regulamentul privind accesul la reţeaua Intranet/Internet şi utilizarea aplicaţiilor software, prevede următoarele reguli privind accesul la email:

1. 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 iniţială, care va fi schimbată de utilizator la prima accesare a contului;
2. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces şi datele din acestea;
3. Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc Universitatea, folosind conturi utilizator care nu sunt proprietatea Universităţii. Exemple de astfel de conturi sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, Gmail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi Furnizori de Servicii Internet.

De asemenea, privind accesul la reţeaua Intranet/Internet şi utilizarea aplicaţiilor software, în vederea accesului la email, sunt interzise următoarele:

1. Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
2. Folosirea sistemului de mesagerie electronică în scopuri personale;
3. Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
4. Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
5. Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ;
6. Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia.

Biroul IT asigură confidenţialitatea datelor personale sau a accesului la informaţii folosind poşta electronică sau alte instrumente de conversaţie electronică în limitele competentelor, a posibilităţilor tehnice existente şi a limitelor impuse de prevederile legale în vigoare.

5.2. Reglementari privind securitatea datelor

Securizarea serverelor se realizează prin următoarele reguli:

1. Serverele trebuie să fie într-o locație cu acces securizat; accesul este restricționat doar la personalul tehnic autorizat;
2. Instalarea sistemului de operare dintr-o sursă aprobată;
3. Setarea/activarea sistemelor de securitate (de tip firewall, IPS antivirus), a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare;
4. Dezactivarea sau schimbarea parolelor conturilor predefinite;
5. Crearea și utilizarea copiilor de siguranță (backup).

Regulile privind parolele de acces sunt următoarele:

1. 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 (%$#&^* …);
2. Nu folosiți aceeași parolă pentru mai multe conturi;
3. 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. parolelemele.rar);
4. Evitați să păstrați parole în agende electronice, telefoane mobile;
5. Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile;
6. 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;
7. Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaților care răspund de securitatea sistemelor informatice;
8. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat;
9. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul locale;
10. Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parole.

În cadrul rețelei UAB sunt interzise următoarele activități:

1. Activități comerciale neautorizate;
2. Trafic masiv de informații sau trafic de informații cu caracter frivol, obscen și pornografic;
3. Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizați;
4. Ștergerea sau alterarea datelor altor utilizatori;
5. Tentativele de descoperire și de folosire a parolelor altor utilizatori;
6. Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;
7. Provocarea deliberată de defectiuni hardware și software;
8. Perturbarea traficului rețelei Universității;
9. Generarea de trafic neacademic;

10. Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică, cărţi, etc.);
11. Generarea de spam;
12. Flood (indiferent de natura acestuia), de exemplu: ping flood;
13. Răspândirea de aplicaţii de tip virus, troieni, viermi, spyware sau altele;
14. Folosirea de aplicaţii de tip key-logere;
15. Modificarea adresei MAC a plăcii de reţea;
16. Setările pentru IP şi DNS, altfel decât cu "Obtain an IP/DNS address automatically", fără autorizaţie din partea Biroului IT;
17. Utilizarea de programe pentru scanarea reţelei, exploit-uri;
18. Transmiterea de mesaje cu caracter comercial;
19. Publicitatea cu caracter comercial;
20. Folosirea de software fără licenţă pe calculatoarele din Universitate sau conectate la reţeaua Universităţii.

5.3. Reglementări/procedee de administrare a informaţiilor

Reguli de administrare a conturilor de email:

1. Fiecare cont de email creat pe domeniul **uab.ro** trebuie să aibă asociate o cerere şi o aprobare corespunzătoare;
2. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces;
3. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat;
4. Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulile privind Parolele de Acces;
5. Numărul de mesaje din Inbox nu este limitat;
6. La cererea conducerii Universităţii, Biroul IT trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

6. Măsuri disciplinare

Administratorul reţelei are dreptul să ia măsuri de restricţionare (blocare parţială sau totală), fără notificare, a accesului la Resursele Informatice şi de Comunicaţii în cazul utilizatorilor care încalcă prevederile acestui regulament sau legislaţia în vigoare şi care, astfel, pun în pericol funcţionarea şi/sau securitatea reţelei UAB.

În situaţii cu totul deosebite, când eventuale acţiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea reţelei, se pot lua următoarele măsuri:

1. rezilierea contractului de muncă în cazul angajaţilor;
2. încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, furnizorilor sau consultanţilor;
3. suspendarea sau exmatricularea în cazul studenţilor.

Toate acţiunile care contravin legilor vor fi raportate conducerii Universităţii.

7. Dispoziţii finale

Aprobarea Regulamentului privind utilizarea reţelei de calculatoare din cadrul UAB se face de către Senatul Universităţii „1 Decembrie 1918" din Alba Iulia.

Prezentul Regulament intră în vigoare la data de 27.11.2019, odată cu aprobarea acestuia de către Senatul Universităţii „1 Decembrie 1918" din Alba Iulia.

În desfăşurarea activităţilor care fac obiectul prezentului regulament se vor respecta reglementările europene impuse de REGULAMENTUL nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), cele naţionale transpuse prin Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 şi reglementările interne elaborate în cadrul Universităţii „1 Decembrie 1918" din Alba Iulia (Regulamentul privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date, aplicabil în cadrul Universităţii „1 Decembrie 1918" din Alba Iulia, politici de confidenţialitate).

Aprobat în Şedinţa Senatului Universităţii „1 Decembrie 1918" din Alba Iulia, din 27 noiembrie 2019.

PREŞEDINTE
Conf. univ. dr. Lucian Marina

ROMÂNIA Universitatea „1 Decembrie 1918" din Alba Iulia SENAT MINISTERUL EDUCAŢIEI NAŢIONALE

AVIZAT
Oficiul Juridic
Consilier juridic Claudia Rotar