Anexa 53
H.S. 36/29.09.2022

UNIVERSITATEA DIN ORADEA

REGULAMENT PRIVIND UTILIZAREA ŞI SECURIZAREA RESURSELOR INFORMATICE ŞI DE COMUNICAŢII ALE UNIVERSITĂŢII DIN ORADEA

	Structura Emitentă	Nume Prenume	Semnătura	Data
Elaborat	SMIIT	Popescu Daniela		05.09.2022
Verificat	DAC	Bandici Livia		09.09.2022
Avizat	Consiliul de Administraţie	Bungău Constantin		21.09.2022
Aprobat	Senatul Univ. din Oradea	Căuş Vasile Aurel		29.09.2022
Ediţia: I				
Intrat în vigoare la data de:				
Retras la data de:				

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE:
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

CAPITOLUL I
DISPOZIŢII GENERALE

Art. 1 Regulamentul privind utilizarea şi securizarea Resursele Informatice şi de Comunicaţii ale Universităţii din Oradea (**R-RIC-UO**) are drept scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei şi stabileşte cadrul necesar pentru elaborarea *Procedurii pentru copiile de rezervă*, a *Procedurii de operare pentru situaţia incidentelor de securitate* şi a *Politicii de utilizare a cookie-urilor*.

Art. 2 Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate folosind sistemul Resurselor Informatice şi de Comunicaţii (**RIC**) propriu, administrate sau în custodia şi sub controlul Universităţii din Oradea sunt confidenţiale şi pot fi accesate de către angajaţii autorizaţi din cadrul Serviciului Management Integrat IT, Departamente / Departamente şi Facultăţi numai în condiţiile prevăzute de lege.

Art. 3 Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

Art. 4 Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor RIC. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a RIC.

Art.5 În acord cu prevederile din prezentul document, RIC puse la dispozitie şi administrate de Serviciul Management Integrat IT (**SMIIT**) sunt bunuri strategice ale Universităţii din Oradea care trebuie administrate ca resurse ale statului român.

Art.6 Compromiterea securităţii acestor resurse poate afecta capacitatea Universităţii din Oradea 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. Aceast regulament este stabilit astfel încât:

a) să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice;

b) să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Universităţii din Oradea;

c) să instruiască utilizatorii care pot folosi legal RIC cu privire la drepturile si responsabilităţile asociate unei astfel de utilizări.

DOCUMENTE DE REFERINŢĂ

1. http://dcd.uaic.ro
2. http://www.uaiasi.ro/diacd/
3. http://www.dict.uvt.ro
4. http://www.usamvcluj.ro/CIC
5. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
6. ISO 17799 – Standard detaliat de securitate:
7. Legea 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.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CAUS

8. Legea nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.
9. Legea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal
10. Legea nr. 455 din 18 iulie 2001 privind semnătura electronică.
11. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
12. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
13. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
14. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.
15. http://anpd.gov.ro/web/conditii-de-utilizare-politica-cookies/
16. https://ec.europa.eu/info/cookies_ro
17. https://razvanbb.ro/template-politica-privind-fisierele-cookies

ABREVIERI

R-RIC-UO	*Regulament privind utilizarea și securizarea Resurselor Informatice şi de Comunicaţii ale Universităţii din Oradea*
RIC	*Resursele Informatice şi de Comunicaţii*
SMIIT:	*Serviciul Management Integrat IT al Universităţii din Oradea*
RIC:	*Resurse Informatice şi de Comunicaţii*
ARIC:	*Administratorul Resurselor Informatice si de Comunicare*
ERIS:	*Echipă de Răspuns la Incidentele de Securitate a RIC*
OSRIC:	*Ofiter responsabil cu Securitatea RIC*
WWW :	*World Wide Web*
LAN:	*Local Area Network*
URL:	*Uniform Resource Locator*
URI:	*Uniform Resource Identifier*
HTTP:	*Hypertext Transfer Protocol*
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
FTP:	*File Transfer Protocol*

DEFINIŢII

Resurse Informatice şi de Comunicaţii (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri),

calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Inginerul de sistem/Administratorul de reţea este şi Administratorul Resurselor Informatice si de Comunicare (ARIC): Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea.

Utilizator: o persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii.

Abuz de privilegii: orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Universităţii din Oradea şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

Furnizor: persoană fizică/juridică care oferă bunuri sau servicii Universităţii din Oradea în baza unui contract comercial sau de colaborare.

Server Web: un sistem de calcul care distribuie în mod public sau diferenţiat informaţii folosind protocolul HTTP.

Pagină web: Un document în spaţiul World Wide Web (WWW). Fiecare pagină web este identificată printr-un URL (*Uniform Resource Locator*).

Echipă de Răspuns la Incidentele de Securitate a RIC (ERIS): personalul responsabil de acţiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate.

Virus: un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte deranjante, sau chiar distructive. Un virus se executa în momentul în care este accesat un fişier infectat. Un virus macro infectează codul executabil încapsulat în pachetul de programe *Microsoft Office* (*Word, Excel, PowerPoint*) sau alte programe care permit utilizatorului să genereze macro-uri.

Vierme: un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descrie un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.

Cal troian: de obicei este un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.

Incident de Securitate: în termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau

confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

Reţea locală (LAN): O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori

Atac informational: o încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informaţiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate.

Protecţie informaţională: acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.

Gazdă (Host): un sistem care oferă servicii pentru un anumit număr de utilizatori.

Server: un program care oferă servicii altor programe aflate pe acelaşi sistem de calcul sau pe alte sisteme conectate în reţea. Un sistem de calcul care rulează un program de tip server este adesea numit server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

Firewall: un mecanism de control al accesului care acţionează ca o barieră între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

Copii de Siguranţă (*backup*): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Stocarea Externă (*Offsite*): Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de campus-ul universitar în care este puţin probabil să se producă efecte de acelaşi tip în cazul unui dezastru. Pe baza unei evaluări a informaţiei pentru care s-au realizat copii de siguranţă, mutarea mediilor de backup din clădire şi depozitarea lor într-o altă zonă securizată din campusul Universităţii din Oradea poate înlocui stocarea externă.

Internet: reprezintă un sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.

Intranet: este o reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (*firewall*).

Parole complexe: o parolă complexă este un şir de caractere (secvenţă de caractere, numere şi caractere speciale) care nu poate fi asociată cu informaţia publică despre contul utilizator, nu este copiată dintr-un dicţionar etc.

Sistem de Mesagerie Electronică: reprezintă orice program care permite ca mesajele în format electronic să fie transmise de la un sistem de calcul la altul.

Mesagerie Electronică: reprezintă orice mesaj, imagine, formular, ataşament, date sau orice alt mijloc de comunicaţie, trimise, primite sau stocate într-un sistem de mesagerie electronică.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

CAPITOLUL II
CLASIFICAREA INFORMAŢIILOR

Art.7 Clasificarea informaţiilor

a) Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât şi pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

b) Pentru a asigura securitatea şi integritatea informaţiilor, acestea se împart în trei categorii principale:

- Publice;
- Secrete;
- Strict Secrete.

Art.8 Serviciul Management Integrat IT şi conducerea Facultăţilor / Departamentelor / Centrelor răspund de evaluarea periodică a schemei de clasificare a informaţiilor. Toate informaţiile din Universitatea din Oradea trebuie să se regăsească în una din următoarele categorii:

a) **Publice**:

- Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul Universităţii din Oradea.
- Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituţiei sau aceste efecte sunt nesemnificative.
- Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele Universităţii din Oradea.

Exemple: Informaţiile de pe aviziere, servere web publice, ştirile de presă, informările Rectorului sau Senatului.

b) **Secrete**:

- În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Se includ aici şi informaţiile pe care Universitatea din Oradea trebuie să le protejeze conform legislaţiei în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice.
- Aceste date vor fi copiate şi distribuite în cadrul Universităţii din Oradea doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

Exemple: clauze contractuale, conturi si parole folosite pe serverele de contabilitate sau gestiune a şcolarităţii.

c) **Strict Secrete sau Confidenţiale:**

- În această categorie se include toate informaţiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale.
- Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii Universităţii.

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

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

CAPITOLUL III
AUDIENŢĂ

Art. 9 Regulamentul privind utilizarea şi securizarea RIC ale Universităţii din Oradea (R-RIC-UO)

a) se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.

b) Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Regulamentului:

- angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- colaboratorii Universităţii din Oradea care au acces la RIC;
- furnizorii Universităţii din Oradea care au acces la RIC;
- studenţii Universităţii din Oradea;
- alte persoane, entităţi sau organizaţii care au acces la RIC.

Art. 10 Atribuţii şi responsabilităţi manageriale privind respectarea R-RIC-UO

- orice angajat sau compartiment al Universităţii din Oradea trebuie să se asigure că managementul respectă prevederile prezentului Regulament şi a regulamentelor sau procedurilor asociate.
- compartimentul de audit intern este responsabil de evaluarea schemei de clasificare a informaţiilor.
- administratorii de reţea / sistem / baze de date trebuie să asigure existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform regulamentelor sau procedurilor asociate.
- administratorii de reţea / sistem / baze de date trebuie să asigure activarea tuturor mecanismelor de securitate.
- administratorii de reţea / sistem / baze de date elaborează şi propun modificări ale politicii de securitate a sistemului RIC[1].
- administratorii de reţea / sistem / baze de date elaborează şi propun pentru aprobare regulamentele şi procedurile de securitate a RIC în conformitate cu politica de securitate a acestora[1].
- administratorii de reţea / sistem / baze de date elaborează proceduri pentru identificarea utilizatorilor RIC[1].
- administratorii de reţea / sistem / baze de date tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra RIC[1].
- administratorii de reţea / sistem / baze de date facilitează evaluările legale ale cerinţelor de tip "cele mai bune practici" pe măsură ce acestea devin recunoscute[1].

Atribuţii ale utilizatorilor:

- să cunoască şi să respecte prevederile Regulamentului privind RIC ale Universităţii din Oradea.
- să cunoască şi să respecte prevederile tuturor Regulamentelor şi/sau Procedurile privind securitatea RIC.

[1] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

- să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

Alte atribuţii:

- Toţi partenerii Universităţii din Oradea (furnizori, agenţi, colaboratori etc.) trebuie să accepte şi să respecte prezentul document.

CAPITOLUL IV
REGULI DE UTILIZARE ACCEPTABILĂ A RESURSELOR INFORMATICE ŞI DE COMUNICAŢII

Art.11 Utilizarea Resurselor Informatice şi de Comunicaţii

a) În acord cu prevederile prezentului Regulament, Resursele Informatice şi de Comunicaţii (RIC) sunt bunuri strategice ale Universităţii din Oradea care trebuie administrate ca resurse ale statului român. Acest regulament este stabilit astfel încât:

(1) Să fie în conformitate cu politicile de securitate, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice;

(2) Să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Universităţii din Oradea;

(3) Să instruiască utilizatorii care au dreptul de folosire a RIC privind responsabilităţile lor asociate unei astfel de utilizări.

b) Regulamentul de Utilizare a Resurselor Informatice şi de Comunicaţii al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

Art. 12 Reguli de utilizare acceptabilă a RIC

- se face numai în interes de serviciu.
- utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
- utilizatorii trebuie să anunţe Serviciul Management Integrat IT atât despre orice problemă/breşă în sistemul de securitate din cadrul Universităţii din Oradea, cât şi despre orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
- prin acţiunile lor, utilizatorii nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul RIC a Universităţii din Oradea.
- utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: *Smartcard*) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.
- utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală si a dreptului de autor (*copyright*).
- utilizatorii nu trebuie să utilizeze programe de tip *shareware* sau *freeware*, fără aprobarea Serviciului Management Integrat IT, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Universităţii din Oradea. Această listă va fi întocmită de către Departamente / Centre şi Facultăţi, aprobată de către Serviciul Management Integrat IT şi publicată de către Departamente / Centre şi Facultăţi.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

• utilizatorii nu trebuie să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane, să degradeze performanțele sistemelor ce alcătuiesc RIC, să împiedice accesul unui utilizator autorizat la RIC, 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 alcătuiesc RIC. De exemplu, utilizatorii UO nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.

• RIC ale Universității din Oradea nu trebuie să fie folosite pentru beneficiul personal.

• utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Universitatea din Oradea 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 RIC se supune aceloraşi reglementări care se aplică utilizării din interiorul instituției și în conformitate cu Art. 25 din prezentul regulament.

• angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la Resursele Informatice și de Comunicații ale Universității.

• utilizatorii care au acces la RIC ale Universității din Oradea 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 desfăşurate prin intermediul sau folosind RIC ale Universității din Oradea.

• utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Universității din Oradea folosind RIC.

• nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Universității din Oradea sau prejudicierea, indiferent de formă, a intereselor Universității.

• în scopul administrării și pentru asigurarea securității RIC, personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activității utilizatorilor în limitele și conform procedurilor prevăzute de legislația în vigoare.

Art. 13 Utilizarea ocazională a Resurselor Informatice și de Comunicații

În anumite situații este permisă utilizarea ocazională a RIC. În aceste situații se aplică următoarele restricții:

• utilizarea personală ocazională a serviciilor de poștă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare etc. este restricționată la utilizatorii autorizați și nu poate fi extinsă la membrii familiilor sau alte persoane;

• utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Universitate;

• utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaților.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29 SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

CAPITOLUL V
CONFIDENȚIALITATEA SERVICIILOR INFORMATICE ȘI DE COMUNICAȚII

Art. 14 Asigurarea confidențialitatii

a) Fișierele electronice create, trimise, primite sau stocate folosind sistemul RIC proprii, administrate sau în custodia și sub controlul Universității din Oradea sunt confidențiale și pot fi accesate de către angajații autorizați din cadrul Serviciului Management Integrat IT, Departamente / Centre și Facultăți numai în condițiile prevăzute de lege.

b) În scopul administrării Resurselor Informatice și de Comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (dar fără a se limita) la numere de telefon formate sau site-uri web vizitate).

c) Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universității din Oradea, orice incident de posibilă întrebuințare greșită sau încălcare a acestui regulament (prin contactarea Serviciului Management Integrat IT).

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

e) Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universitatii din Oradea pentru care nu au autorizație sau consimțământ explicit.

f) Nici un utilizator al sistemului RIC a Universității din Oradea nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun RIC. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Universitatea din Oradea.

g) 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 din Oradea se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

Art. 15 Confidențialitatea Serviciilor Informatice și de Comunicații

a) Reglementările privind confidențialitatea sunt mecanisme utilizate pentru a stabili limite pentru utilizatorii RIC. Confidențialitatea informației este asigurată în cadrul RIC ale Universității din Oradea în condițiile legislației în vigoare. Utilizatorii externi ar trebui să se aștepte la confidențialitate totală, cu excepția cazului în care se suspectează un delict cu privire la sistemul RIC.

b) Scopul reglementărilor privind Confidențialitatea Serviciilor Informatice și de Comunicații ale Universității din Oradea este acela de a comunica în mod clar utilizatorilor prevederile referitoare la confidențialitatea datelor stocate în sistemul RIC.

c) Reglementările privind Confidențialitatea Serviciilor Informatice și de Comunicații ale Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a Universității din Oradea.

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

Art. 15.1 Accesul Publicului la Informații

a) Jurnale și Monitorizare: Universitatea din Oradea păstrează fișierele cu înregistrări ale tuturor accesărilor sit-urilor sale și de asemenea monitorizează traficul din rețea în scopul administrării site-urilor. Această informație este utilizată pentru a ajuta la diagnosticarea eventualelor probleme și pentru a realiza alte sarcini administrative. Uneltele de analiză a jurnalelor sunt de asemenea utilizate pentru statistici în scopul determinării informației cu un grad ridicat de interes pentru utilizatori sau vizitatori. Informațiile incluse în aceste fișiere sunt:

- *numele sistemului:* numele sistemului și/sau adresa IP a calculatorului care cere accesarea sit-ului.
- *Agent-Utilizator:* tipul browser-ului, versiunea, și sistemul de operare al calculatorului care cere accesarea site-ului
- *Referință:* pagina web de unde a venit utilizatorul.
- *Data sistemului:* data și ora accesării.
- *Cerere completă:* cererea exactă făcută de utilizator.
- *Stare:* codul de stare returnat de server, ex: "*file not found*" (nu a găsit fișierul).
- *Mărimea conținutului:* lungimea, în bytes (octeți), a fișierului trimis utilizatorului.
- *Metodă:* metoda cererii folosită de către browser (ex.: post, get).
- *Uniform Resource Identifier (URI):* adresa unei anumite resurse cerute.
- *Șir de interogare din URI:* orice după un semn de întrebare în cadrul unui URI. De exemplu, dacă a fost cerut un cuvânt cheie de căutare, acel cuvânt cheie va apare în șirul interogării.
- *Protocol:* protocolul tehnic și versiunea utilizată, de ex.: http 1.0, ftp, etc.

b) Informația de mai sus nu va fi folosită pe nici o cale care ar putea dezvălui informație de identificare personală unei persoane din exteriorul Universității din Oradea, decât dacă se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale. De asemenea este interzisă utilizarea informației de către administratorii sistemului IT în alte scopuri decât cele privind administrarea sistemului, respectiv de prevenire a activităților ilegale sau imorale.

c) Informație din mesaje electronice sau formulare: Dacă un vizitator trimite un mesaj electronic Universității din Oradea sau completează un formular web cu o întrebare sau comentariu ce conține informație de identificare personală, aceea informație va fi utilizată numai pentru a răspunde cererii și pentru a analiza intențiile. Mesajul poate fi redirecționat la altă persoană care este calificată să răspundă cererii. Astfel de informații nu vor fi folosite pe nici o cale prin care s-ar dezvălui informație de identificare personală terților, cu excepția cazului în care Universității i se cere în mod legal acest lucru în conformitate cu legile în vigoare sau cu alte proceduri legale.

d) Legături: Acest site poate conține legături la alte site-uri. Universitatea din Oradea nu este răspunzătoare de politicile de securitate sau conținutul acestor site-uri.

e) Contact: Pentru informații privind utilizarea acestui site vă rugăm să ne contactați.

Art.15.2 Acces la Rețeaua de Comunicații

a) Rețeaua de comunicații a Universității din Oradea constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuție și nodurile principale. Este important ca aceasta să se dezvolte controlat și continuu în condiții de flexibilitate și evolutivitate. Este important ca dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate și diferențiate cât și cerințele privind securitatea întregului ansamblu.

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

b) Scopul reglementărilor privind accesul la Rețeaua de Comunicații a Universității din Oradea constă în stabilirea regulilor de acces și utilizare a acesteia. Aceste reguli sunt necesare pentru păstrarea integrității, disponibilității și confidențialității informației din cadrul RIC ale Universității din Oradea.

c) Accesul la Rețeaua de Comunicații a Universității din Oradea se aplică nediscriminatoriu tuturor utilizatorilor care au acces la orice RIC.

d) Accesul la Rețeaua de Comunicații constă în următoarele:

- Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la rețea specificați de către Serviciul Management Integrat IT.
- Departamentele / Centrele și Facultățile trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale Universității. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele și datele de identificare ale acesteia se vor comunica către Serviciul Management Integrat IT.
- Utilizatorii RIC din interiorul Universității nu se pot conecta la altă rețea.
- Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în nici un fel, pe nici o cale. Nu este permisă instalarea de conexiuni de rețea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăților / Centrelor și a Departamentelor de către Serviciul Management Integrat IT.
- Sistemele computerizate din afara Universității care necesită conectare la rețea trebuie să se conformeze cu standardele rețelei interne ale Universității.
- Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii Universității nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectați la rețeaua Universității.
- Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, cabluri, prize de conexiuni.
- Serviciul de nume și administrarea adreselor IP sunt deservite exclusiv de către Serviciul de Management Integrat IT.
- Serviciile de interconectare a rețelei Universității din Oradea cu alte rețele sunt realizate exclusiv de către Serviciul de Management Integrat IT.

e)Nu este permisă instalarea și/sau modificarea echipamentelor utilizate pentru conectare la rețea (inclusiv plăci de rețea) fără aprobarea Serviciul de Management Integrat IT.

Art. 16 Cookie-uri

Un "cookie" este un fișier care conține informație plasată de către un server web pe un calculator al utilizatorului. De obicei, aceste fișiere sunt utilizate pentru a facilita accesul la informația oferită de site-ul web. Orice informație pe care serverele web ale Universității din Oradea o pot stoca în cookie-uri este utilizată numai în interiorul UO. Informația din cookie-uri nu este utilizată pentru a dezvălui, către terți, informații despre vizitator decât în cazul în care Universității din Oradea i se cere în mod legal să facă acest lucru în conformitate cu legile în vigoare sau alte proceduri legale.

Art.17 Accesul Administrativ

a) Personalul care asigură suport tehnic, administratorii de sistem și alte persoane pot avea conturi cu drepturi de acces privilegiat în comparație cu utilizatorii obișnuiți. Datorită faptului că

aceste conturi pentru acces administrativ au mai multe privilegii, aprobarea, verificarea şi monitorizarea acestora sunt extrem de importante din punctul de vedere al securităţii RIC.

b) Scopul reglementărilor privind accesul administrativ este de a stabili regulile pentru crearea, utilizarea, monitorizarea, controlarea şi ştergerea conturilor cu drepturi speciale de acces.

c) Reglementările se aplică nediscriminatoriu tuturor persoanelor care au sau pot cere şi obţine drepturi speciale de acces la orice RIC ale Universităţii din Oradea.

d) Utilizatorii trebuie să cunoască şi să accepte toate reglementările privind securitatea RIC înainte de a li se permite accesul la un cont.

e) Utilizatorii care au conturi de acces administrativ trebuie să aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare Departament / Centru sau Facultate şi vor fi incluse în fişa postului.

f) Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea Inginerului de sistem/ Administratorului de reţea.

g) Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.

h) Accesul administrativ trebuie să se conformeze reglementărilor pentru Parolele de acces.

i) Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al Serviciului Management Integrat IT şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului / Centrului, Facultăţii sau a Universităţii, sau în cazul unei modificări a listei de personal a terţilor (furnizor desemnat) în contractele cu Universitatea din Oradea.

j) Pentru cazuri de forţă majoră accesul cu drept de administrator la resursele RIC ale Universităţii se va face conform unei proceduri de acţionare în situaţii de incident de securitate.

k) Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:

- trebuie să fie autorizate;
- trebuie create cu dată de expirare specifică;
- contul va fi şters atunci când nu mai este necesar.

Art.18 Accesul fizic la Resursele Informatice şi de Comunicaţii

a) Personalul care asigură suport tehnic, administratorii de reţea, administratorii de sistem sau alte persoane autorizate trebuie să aibă acces la echipamentele şi componentele sistemului *Resurse Informatice şi de Comunicaţii* (RIC). Procesul de control şi monitorizare a drepturilor de acces fizic la resursele RIC este important şi va fi reglementat conform prezentului regulament de către Serviciul Management Integrat IT şi, acolo unde este cazul, de către fiecare Departament / Centru sau Facultate.

b) Scopul reglementării privind Accesul Fizic la RIC este stabilirea regulilor pentru acordarea, controlarea, monitorizarea şi întreruperea drepturilor de acces fizic la echipamentele componente ale RIC.

c) Reglementarea privind Accesul Fizic la RIC se aplică tuturor persoanelor care răspund de buna funcţionare a infrastructurii, instalarea şi întreţinerea unor componente funcţionale, a personalului responsabil cu securitatea RIC şi utilizatori.

d) Reglementări privind accesul fizic la Resursele Informatice şi de Comunicaţii:

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

- Toate sistemele de securitate fizică a Resurselor Informatice şi de Comunicaţii (RIC) – cum ar fi, de exemplu: coduri de acces în clădire şi coduri de acces pentru prevenirea incendiilor - trebuie să fie instalate în conformitate cu regulamentele Universităţii.
- Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
- Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
- Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
- Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
- Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face în scris de către Serviciul Management Integrat IT sau, după caz, Departamentul / Centrul sau Facultatea care deţine încăperea şi resursele.
- Nu este permis transferul dreptului de acces indiferent de motiv.
- Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate Departamentului / Centrului sau Facultăţii care le-a eliberat.
- Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat Departamentului / Centrului sau Facultăţii care le-a eliberat.
- Cardurile şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare.
- Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare încăpere şi, în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat.
- Fiecare Departament / Centru şi Facultate va ţine o evidenţă a tuturor cardurilor şi/sau cheilor de acces emise, retrase, pierdute sau furate.
- Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

Art.19 Tratarea incidentelor de securitate

a) Reţeaua de comunicaţii a Universităţii din Oradea constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuţie şi nodurile principale. Este important ca aceasta să se dezvolte controlat şi continuu în condiţii de flexibilitate şi evolutivitate. Este important ca dezvoltarea reţelei de comunicaţii să se facă având în vedere atât cerinţele utilizatorilor privind furnizarea de servicii avansate şi diferenţiate cât şi cerinţele privind securitatea întregului ansamblu.

b) Procedura pentru situaţia incidentelor de securitate va descrie cerinţele şi regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate. Acestea includ (dar nu sunt limitate la): detectarea programelor de tip virus, vierme informatic etc., folosirea neautorizată a conturilor de acces şi a calculatoarelor în sine, precum şi reclamaţiile privind folosirea improprie a RIC după cum este subliniat în regulamente.

c) Procedura pentru situaţia incidentelor de securitate se va aplica nediscriminatoriu tuturor persoanelor care folosesc orice componentă a RIC.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

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

e) Ori de câte ori un incident de securitate este suspectat sau confirmat (exemple: virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc.), trebuie urmată Procedura de operare pentru situaţia incidentelor de securitate.

f) Serviciul Management Integrat IT este responsabil cu înştiinţarea şi coordonarea pentru tratarea incidentului.

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

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

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

j) Serviciul Management Integrat IT trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.

k) Serviciul Management Integrat IT este responsabil cu documentarea anchetei privind incidentul.

l) Serviciul Management Integrat IT este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

m) În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare Serviciul Management Integrat IT va recomanda sancţiuni disciplinare.

n) În cazul în care incidentul implică aplicarea legilor civile sau penale, Serviciul Management Integrat IT va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

Art.20 Monitorizarea Resurselor Informatice şi de Comunicaţii

a) Monitorizarea RIC pentru asigurarea securităţii sistemului este o metodă utilizată pentru a confirma funcţionalitatea şi eficienţa măsurilor de securitate. Această activitate constă în următoarele (fără a se limita numai la aceste exemple):

- Detectarea automată a intruşilor prin intermediul sistemelor de înregistrare (logare);
- Jurnale *Firewall;*
- Jurnale ale activităţii conturilor utilizator;
- Jurnale ale scanărilor reţea;
- Jurnale ale aplicaţiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme şi servere.

b) Scopul monitorizării RIC este stabilirea regulilor şi procedurilor pentru verificarea funcţionalităţii şi eficienţei măsurilor de securitate. De asemenea această activitate urmăreşte detectarea situaţiilor de evitare sau dezactivare a controalelor. Unul din beneficiile monitorizării securităţii este identificarea din timp a tentativelor de fraudă sau a infracţiunilor şi a vulnerabilităţilor sistemelor componente ale RIC. Alte beneficii includ: rezolvarea reclamaţiilor, monitorizarea serviciilor, estimarea performanţelor sistemelor în vederea întocmirii planurilor de modernizare, etc.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

c) Reglementările privind monitorizarea RIC ale Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a Universității din Oradea.

d) Monitorizarea Resurselor Informatice și de Comunicații (RIC) se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări și înregistra:

- Tipul traficului (ex. structura pe protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Tipul protocoalelor și a echipamentelor conectate la RIC, conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

e) Fișierele jurnal, vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentele de securitate ale Universității. În această categorie intră următoarele (fără a se limita doar la acestea):

- Jurnale ale sistemelor de detectare automată a intruşilor;
- Jurnale *Firewall*;
- Jurnale ale activității conturilor utilizator;
- Jurnale ale scanărilor rețea;
- Jurnale ale aplicațiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme și servere.

f) Serviciul Management Integrat IT, sau personalul autorizat al Departamentelor / Centrelor sau Facultăților, va efectua, în mod regulat (cel puțin o dată la șase luni), verificări pentru detectarea:

- Echipamentelor de rețea conectate neautorizat;
- Parolelor utilizator care nu respectă regulamentele;
- Serviciilor de rețea neautorizate;
- Serverelor de pagini web neautorizate;
- Echipamentelor ce utilizează resurse comune nesecurizate;
- Utilizării de modem-uri neautorizate;
- Licențelor pentru sistemele de operare și programele instalate.

g) Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Serviciul Management Integrat IT în scopul efectuării de investigații.

Art.21 Detectarea Accesului Neautorizat

a) Detectarea tentativelor de acces neautorizat este o prioritate la nivelul SMIIT din cadrul Universității din Oradea. Pe măsură ce complexitatea sistemelor informaționale și de comunicații crește, sistemele de securitate trebuie să evolueze. Odată cu creșterea numărului de vulnerabilități prin utilizarea sistemelor distribuite este necesar un mecanism de asigurare a securității la nivel de sistem precum și la nivel de rețea. Sistemele de detectare a accesului neautorizat pot contribui la atingerea acestui scop.

b) Detectarea tentativelor de acces neautorizat furnizează două funcții importante pentru protejarea resurselor informatice:

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

- *Feedback,* informații referitoare la eficiența componentelor din sistemul de securitate. Dacă nu se detectează tentative sau chiar acces neautorizat în condițiile în care se folosește un sistem de detectare se consideră că mecanismele de apărare funcționează.

- *Trigger,* un mecanism automat care determină când este necesară activarea anumitor măsuri specifice ca răspuns la un incident privind accesul neautorizat.

c) Reglementările privind detectarea tentativelor de acces neautorizat în sistemul RIC al Universității din Oradea, se aplică tuturor persoanelor responsabile de instalarea de noi RIC precum și persoanelor care răspund de utilizarea RIC existente și persoanelor însărcinate cu Securitatea RIC.

d) Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).

e) Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de *firewall*-uri și sistemele de control al accesului la rețea.

f) Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele *firewall* și pe toate sistemele de control al accesului.

g) Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate / revizuite (examinate) zilnic de către administratorul de sistem.

h) Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie și pentru dispozitivele de tip *firewall* sau dispozitive de control al accesului.

i) Înregistrările de verificare pentru serverele și host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal.

j) Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.

k) Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

l) Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Serviciul Management Integrat IT.

m) Utilizatorii sunt obligați să raporteze Serviciului Management Integrat IT orice anomalii în performanța sistemelor utilizate sau orice semne ale unor posibile infracțiuni.

Art. 22 Crearea și utilizarea copiilor de siguranță (backup)

a) Copiile de siguranță (*backup*) sunt necesare pentru a permite recuperarea datelor și aplicațiilor în cazul unor evenimente cum ar fi: dezastre naturale, defecțiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcționare a sistemului etc.

b) Scopul Procedurii pentru copiile de siguranță (backup-uri) în Universitatea din Oradea este de a stabili regulile pentru crearea copiilor de siguranță și stocarea informațiilor electronice ale Universității din Oradea.

c) Procedura pentru copiile de siguranță (*backup-uri*) ale Universității din Oradea se aplică tuturor persoanelor din cadrul Universității din Oradea care sunt responsabile cu instalarea și întreținerea de RIC, persoanelor însărcinate cu securitatea RIC și deținătorilor de informații.

d) SMIIT, administratorul RIC poate avea contracte pentru stocarea copiilor de siguranță (*backup*) în alte zone. Aceste servicii pot fi extinse, la cerere, către toate Departamentele / Centrele și Facultățile din Universitatea din Oradea.

e) Frecvența, dimensiunea și conținutul copiilor de siguranță trebuie să fie în

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

concordanță cu importanța informației și cu riscul acceptat de proprietarul datelor.

f) Procedura de creare a copiilor de siguranță și de recuperare pentru fiecare sistem din cadrul Resurselor Informatice și de Comunicații trebuie să fie documentată și periodic revizuită.

g) Furnizorul care oferă servicii de stocare a copiilor de siguranță în alte zone pentru Universitate trebuie să fie acreditat în acest scop de către o autoritate a statului.

h) Procedurile stabilite între Universitate și furnizorii de stocare a copiilor de siguranță în altă zonă trebuie să fie revizuite cel puțin anual.

i) Verificarea copiilor de siguranță se va face conform Procedurii pentru copii de siguranță.

j) Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.

k) Accesul la mediile de *backup* ale Universității stocate la furnizori externi sau în interior se va face folosindu-se proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.

l) Benzile sau mediile utilizate pentru stocarea copiilor de siguranță trebuie să aibă un sistem de identificare care să conțină cel puțin următoarele date de identificare a informației stocate:

- numele sistemului;
- data creării copiei;
- tipul de copie (completă, incrementală etc.);
- clasificarea sensibilității (siguranței/securității);
- informații de contact.

Art.23 Securizarea Serverelor

a) Serverele sunt acele sisteme care stochează și distribuie informația către utilizatorii autorizați. În acest context trebuie asigurată integritatea, confidențialitatea și disponibilitatea datelor prin instalarea și menținerea acestora într-o manieră care să prevină accesul neautorizat, utilizarea neautorizată și întreruperea unor servicii

b) Scopul securizării serverelor din Universitatea din Oradea este de a prezenta cerințele de instalare a unui nou server si de a menține integritatea securității acestuia și a aplicațiilor.

c) Reglementările privind modul de Securizare a Severelor Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a Universității din Oradea.

d) Un server va fi conectat la rețeaua Universității din Oradea numai dacă se află într-o stare sigură, acreditată de către Serviciul Management Integrat IT.

e) Procedura de securizare a serverelor trebuie să includă, obligatoriu, următoarele:

- instalarea sistemului de operare dintr-o sursă aprobată;
- aplicarea *patch*-urilor furnizate de producător;
- înlăturarea programelor, a serviciilor sistem și a driver-elor care nu sunt necesare;
- dezactivarea sau schimbarea parolelor conturilor predefinite;
- securizarea accesului fizic la aceste echipamente;
- setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare.

f) Serviciul Management Integrat IT, în colaborare cu administratorii de sistem ai

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

structurilor UO, va monitoriza, în mod obligatoriu, procesul de instalare a serverelor principale (*enterprise*) şi aplicarea regulată a *patch*-urilor de securitate. De asemenea, va monitoriza, prin sondaj, procesul de instalare şi aplicarea regulată a *patch*-urilor de securitate pentru serverele departamentelor / centrelor sau ~~a~~ grupurilor de lucru.

Art.24 Detectarea virușilor

a) Numărul incidentelor de securitate şi costurile ce rezultă din întreruperea şi restabilirea serviciilor RIC sunt în continuă creştere. Câteva dintre acţiunile care pot fi luate pentru reducerea riscurilor şi scăderea costurilor incidentelor de securitate sunt:

- implementarea unor reguli severe de securitate, blocarea accesului inutil la RIC;
- detectarea în timp util şi minimizarea efectelor cauzate de incidente de securitate.

b) Scopul acţiunilor de Detectare a Virușilor din RIC este de a descrie măsuri ce trebuie luate pentru prevenirea, detectarea şi îndepărtarea programelor de tip virus, vierme sau altele asemănătoare.

c) Reglementările privind detectarea virușilor se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

d) Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus.

e) Programele antivirus nu trebuie dezactivate.

f) Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

g) Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

h) Orice server de fişiere conectat la reţeaua instituţiei trebuie să utilizeze un program antivirus în scopul detectării şi curăţirii virușilor care pot infecta fişierele puse la dispoziţie.

i) Orice server sau *gateway* pentru e-mail trebuie să folosească un program antivirus pentru e-mail şi trebuie să respecte regulile de instalare şi de utilizare a acestui program.

j) Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Serviciului Management Integrat IT.

CAPITOLUL VI
REGLEMENTARI PRIVIND UTILIZAREA INTERNET SI INTRANET

Art. 25 Utilizarea reţelei Internet şi Intranet

a) În acord cu prevederile din prezentul Regulament, Resursele Informatice şi de Comunicaţii (RIC) sunt bunuri strategice ale Universităţii din Oradea care trebuie administrate ca resurse ale statului român. Aceste reglementări sunt stabilite pentru a atinge următoarele scopuri:

- să fie în conformitate cu statutul, regulamentele şi alte documente oficiale în vigoare pentru administrarea resurselor informatice;
- să stabilească practici prudente şi acceptabile privind utilizarea reţelei Internet;
- să instruiască utilizatorii care pot folosi reţeaua Internet în ceea ce priveşte responsabilităţile lor asociate unei astfel de utilizări.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

b) Reglementările privind modurile de utilizare Internet şi Intranet se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea care are capacitatea de acces Internet şi/sau Intranet. Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri academice şi de cercetare.

c) Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Serviciul Management Integrat IT. Aceste programe trebuie să includă toate *patch*-urile de securitate puse la dispoziţie de către producător.

d) Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.

e) Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor *Proxy* şi/sau *firewall*.

f) Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze **R-RIC-UO.**

g) Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.

h) Conţinutul tuturor site-urilor web ale Universităţii trebuie să se conformeze **R-RIC-UO.**

i) Nu se vor publica pe site-urile web ale Universităţii materiale cu caracter ofensator sau de hărţuire.

j) Nu se vor publica pe site-urile web ale Universităţii materiale publicitare comerciale sau personale.

k) Nu se vor publica pe sit-urile web ale Universităţii din Oradea date ale Universităţii din Oradea fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.

l) Nu este permisă utilizarea RIC ale Universităţii în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea.

m) Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise.

n) Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie ale Universităţii.

o) Orice material confidenţial al Universităţii transmis prin reţeaua Internet trebuie criptat.

p) Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament / Centru sau Facultate.

Art.25.1 Utilizare ocazională

a) Utilizarea personală ocazională a RIC pentru acces la reţeaua Internet este permisă doar utilizatorilor care au aprobarea Universităţii din Oradea; acest drept nu se extinde membrilor familiei sau altor persoane.

b) Utilizarea ocazională nu trebuie să aibă ca rezultat costuri directe pentru Universitatea din Oradea.

c) Utilizarea ocazională nu trebuie să afecteze îndeplinirea sarcinilor de serviciu ale angajatului sau activitatea studenţilor.

d) Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii din Oradea, sau punerea acesteia într-o situaţie delicată.

e) Stocarea fişierelor şi documentelor personale pe Resursele Informatice ale Universităţii din Oradea, trebuie să fie nominală.

f) Toate fişierele şi documentele – inclusiv cele personale – stocate sau transportate prin intermediul RIC sunt proprietatea Universităţii din Oradea, în condiţiile legilor în vigoare. Acestea pot fi subiectul cererilor de deschidere a raporturilor, şi pot fi accesate în conformitate cu Regulamentul de Acces Administrativ.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

Art. 26 Parolele de acces

a) Autentificarea este necesară pentru a controla accesul utilizatorilor la Resursele Informatice şi de Comunicaţii (RIC). Controlul accesului este necesar deoarece accesul neautorizat poate duce la prejudicii cauzate de afectarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor. Acestea pot avea ca efecte pierderi materiale şi morale pentru Universitatea din Oradea. Autentificarea utilizatorilor se poate realiza folosind diverse metode: conturi şi parole de acces, dispozitive de identificare, caracteristici biologice.

b) Reglementările pentru crearea şi modificarea parolelor de acces la RIC se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

c) Criterii pentru Alegerea unei parole:

- 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 (%$#&^* ...).
- Nu este deloc recomandată folosirea simplă a datelor personale (ex: data naşterii, nume, prenume etc.) ca parole.

d) Parolele trebuie să respecte următoarele condiţii:

- Nu trebuie să coincidă sau să fie asemănătoare cu numele dvs. de utilizator (login-ul);
- Nu trebuie să coincidă sau să fie asemănătoare cu numărul dvs. de angajat;
- Nu trebuie să coincidă sau să fie asemănătoare cu numele dvs.;
- Nu trebuie să coincidă sau să fie asemănătoare cu numele membrilor familiei;
- Nu trebuie să coincidă sau să fie asemănătoare cu o eventuală poreclă (*nickname*);
- Nu trebuie să coincidă cu codul numeric personal;
- Nu trebuie să coincidă cu data naşterii;
- Nu trebuie să coincidă cu numărul de înmatriculare al maşinii;
- Nu trebuie să coincidă cu adresa;
- Nu trebuie să fie numărul dvs. de telefon;
- Nu trebuie să coincidă cu numele oraşului;
- Nu trebuie să coincidă cu numele departamentului etc.;
- Nu trebuie să coincidă cu nume de străzi;
- Nu trebuie să coincidă cu mărci sau modele de maşini;
- Nu trebuie să coincidă cu argouri;
- Nu trebuie să coincidă cu obscenităţi;
- Nu trebuie să fie termeni tehnici;
- Nu trebuie să coincidă cu numele, mascota sau sloganul unei şcoli;
- Nu trebuie să coincidă cu informaţii despre proprietarul contului care sunt cunoscute sau uşor de ghicit (mâncarea, culoarea preferată, sportul preferat etc.);
- Nu trebuie să coincidă cu un acronim popular;
- Nu trebuie să fie cuvinte din dicţionar;
- Nu trebuie să fie opusul tuturor celor de mai sus;
- Parolele nu trebuie să fie reutilizate pentru o perioadă de un an;
- Parolele nu trebuiesc divulgate în nici o situaţie;
- Parolele trebuiesc tratate ca informaţie confidenţială.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

Art. 26.1 Reguli pentru utilizarea parolelor:

a) Toate parolele trebuie să îndeplinească următoarele condiţii:

- Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;
- Să aibă o lungime minimă de 8 caractere;
- Să fie parole complexe;
- Reutilizarea parolelor este interzisă;
- Parolele stocate trebuie criptate;
- Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.

b) Este interzisă notarea parolelor pe hârtii.

c) Nu se foloseşte aceeaşi parolă pentru mai multe conturi.

d) Dacă un utilizator are mai multe parole, acestea se pot scrie într-un fişier care trebuie criptat.

e) Se va evita denumirea acelui fişier cu una explicită (*parolelemele.rar*).

f) Se va evita păstrare parolelor în agende electronice, telefoane mobile – pot fi furate.

g) Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea Inginerului de sistem/Administratorului de reţea.

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

i) Având în vedere că browser-ele au facilitatea de reţinere a parolelor (AutoFill, Remember password), aceasta trebuie dezactivată pe calculatoarele care pot fi folosite de mai multe persoane.

j) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.

k) Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

l) Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.

m) 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.

n) 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.

o) Dispozitivele de securitate (ex. card *Smart*) trebuiesc returnate după terminarea relaţiilor cu Universitatea din Oradea.

Art. 27 Administrarea conturilor de email

a) Conturile utilizator sunt mijloacele utilizate pentru a permite accesul la RIC ale Universităţii din Oradea. Astfel, crearea, modificarea, controlul şi monitorizarea conturilor utilizator sunt operaţiuni foarte importante în cadrul general al asigurării securităţii sistemului RIC.

b) Administrarea conturilor de email din Universitatea din Oradea se face prin stabilirea de reguli pentru crearea, utilizarea, monitorizarea, controlul şi ştergerea acestora.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

c) Administrarea conturilor de email ale Universității din Oradea se aplică nediscriminatoriu tuturor persoanelor care au acces autorizat la sistemul de RIC din cadrul Universității din Oradea

d) Modul de administrare a conturilor de email presupune:

- Toate conturile create trebuie să aibă asociată o cerere și o aprobare corespunzătoare.
- Toate conturile utilizator se vor crea în formatul Prenume.Nume, sau alternative.
- Prin contractul de muncă, contractul de școlarizare și/sau alte documente toți utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.
- Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces.
- Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
- Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu reglementările privind Parolele de Acces.

e) Administratorii de sisteme sau alt personal autorizat:

- Sunt responsabili de ștergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în Universitatea din Oradea, sau care nu mai au relații cu Universitatea din Oradea.
- Trebuie să aibă o documentație de modificare a conturilor utilizator pentru a se pune de acord în situații precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator.
- Sunt subiectul verificării independente.
- Trebuie să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii autorizate din Universitatea din Oradea.

Art. 28 Reglementări privind Sistemul de mesagerie electronică

a) Aceste reglementări sunt stabilite astfel încât:

- să fie în conformitate cu **R-RIC-UO**, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice, al Universității din Oradea;
- să instruiască utilizatorii care au dreptul de folosire a RIC privind responsabilitățile lor asociate unei astfel de utilizări.

b) Scopul acestor reglementări cu privire la Sistemul de Mesagerie Electronică al Universității din Oradea, este de a stabili regulile pentru utilizarea serviciului de poștă electronică din cadrul Universității din Oradea, privind trimiterea, primirea sau stocarea mesajelor asociate poștei electronice.

c) Prezentele reglementările privind Sistemul de Mesagerie Electronică al Universității din Oradea, se aplică nediscriminatoriu tuturor persoanelor care au permisiuni de acces la orice resursă informatică din cadrul Universității care are capacitatea de a trimite, primi sau stoca mesaje asociate poștei electronice.

d) **Activități strict interzise:**

- trimiterea de mesaje cu caracter de intimidare sau hărțuire;
- folosirea sistemului de mesagerie electronică în scopuri personale;
- folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

APROBAT ÎN ȘEDINȚA DE SENAT
DIN DATA DE
29. SEP. 2022
Președinte:
Conf.univ.dr. Vasile-Aurel CĂUȘ

e) **Activităţi interzise** deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:

- trimiterea sau retrimiterea email-urilor în lanţ;
- trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
- trimiterea mesajelor de dimensiuni foarte mari;
- trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.
- ignorarea cererii administratorului reţelei de a elibera spaţiile de pe server pe care le ocupă.

f) Conform reglementarilor cu privire la administrarea conturilor de email, toţi utilizatorii (cu excepţia persoanelor care au funcţii de conducere şi a celor din secretariate) se obligă să menţină în directoarele proprii de pe serverul de mail numai mesajele din cel mult ultimele 14 zile.

g) Toţi utilizatorii sistemului RIC, fără excepţie, vor folosi adrese e-mail din domeniul uoradea.ro (toate adresele e-mail vor avea sufixul uoradea.ro).

h) Toate informaţiile şi datele confidenţiale ale Universităţii, transmise către alte reţele externe, trebuie să fie criptate.

i) Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea resurselor informatice şi de comunicaţii ale Universităţii pot fi oricând înregistrate şi analizate, în condiţiile respectării prevederilor legale privind confidenţialitatea informaţiei.

j) Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele Universităţii, cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă Universitatea. Un exemplu de declaraţie simplă este: "părerile exprimate sunt personale, şi nu ale Universităţii din Oradea"

k) Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc Universitatea din Oradea, folosind conturi utilizator care nu sunt proprietatea Universităţii din Oradea. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea): gmail, Hotmail, Yahoo mail, AOL mail, precum şi adrese de email puse la dispoziţie de alţi Furnizorii de Servicii Internet.

l) Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, care privesc Universitatea din Oradea, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de către aceasta. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: telefoane mobile, asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii.

m) Reţeaua UONet se declară a fi un mediu de lucru şi comunicare academic, deschis şi civilizat. Utilizatorii sunt invitaţi să se trateze reciproc în mod politicos şi cordial. Spiritul Internet presupune dialoguri într-un stil caracterizat prin decenţă, amabilitate şi bunăvoinţă. Partenerii noştri din Internet se aşteaptă să găsească în UO şi un mediu academic atunci când solicită informaţii despre noi, motiv pentru care, utilizatorii vor lua măsuri pentru a se autoidentifica corect atât pe serverul din uoradea, cât şi în corespondenţa electronică pe care o trimit.

CAPITOLUL VII
DISPOZITII FINALE

Art. 29 Măsuri disciplinare

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

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

- În cazul angajaţilor UO, se va proceda la suspendarea accesului la resurse, respectiv la alte măsuri disciplinare – conform legislaţiei în vigoare;
- Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenţilor;
- Interzicerea accesului la Resursele Informatice şi de Comunicaţii;
- Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Art. 30 Alte dispoziţii

Acest Regulament are ca parte integrantă următoarele dispoziţii:

a) întreg personalul este responsabil privind modul de utilizare a RIC; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea RIC.

b) utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament.

c) Utilizarea mesageriei electronice, navigarea Web, conversaţiile telefonice, transmisile prin fax-uri şi alte instrumente de conversaţie electronică pot fi monitorizate de către organele competente, în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.

d) Departamentele/ Centrele şi Facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC;

e) orice informaţie folosită în sistemul RIC trebuie să fie păstrată confidenţială şi în siguranţă de către utilizator. Faptul că informaţiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidenţiale şi în siguranţă, tipul informaţiei sau chiar informaţia în sine stau la baza determinării gradului de siguranţă necesar;

f) toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate;

g) Departamentele / Centrele şi Facultăţile trebuie să ofere facilitate corespunzătoare de control al accesului în scopul monitorizării RIC, protejării datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător;

h) orice program comercial utilizat în cadrul RIC trebuie să fie însoţit de Licenţă care să specifice clar drepturile de utilizare şi restricţiile produsului. Personalul trebuie să respecte prevederile Licenţelor si nu este permisă copierea ilegală a programelor comerciale. Serviciul Management Integrat IT, direct sau prin intermediul Departamentelor / Centrelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIC;

i) inginerii de sistem/Administratorii de reţea, direct sau prin intermediul Departamentelor / Centrelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

Art. 31 Dispoziţii finale

a) Regulamentul privind RIC ale Universităţii din Oradea impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau regulamente specifice. Toate procedurile şi/sau regulamentele de securitate ale RIC fac parte din Planul de Securitate şi sunt obligatorii pentru toţi utilizatorii.

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

b) Serviciul Management Integrat IT are obligaţia de a revizui periodic prezentul Regulament şi de a propune dezvoltarea şi/sau modificarea Planului de Securitate.

c) În contractele de muncă, contractele de şcolarizare cu studenţii şi contractele cu terţii care implică accesul la resursele sistemului Informatic şi de Comunicaţii ale Universităţii, se vor introduce obligatoriu referiri la Regulamentele şi politica de securitate ale RIC.

d) Componentele prezentului regulament vor fi elaborate de către Serviciul Management Integrat IT şi vor fi propuse pentru aprobare conducerii Universităţii din Oradea.

e) Prezentul document va conţine informaţii de identificare proprie, în care se va specifica data la care acesta a fost aprobat şi data de la care intră în vigoare.

f) Prezentul document va fi disponibil în format electronic pe site-ul web al Universităţii din Oradea şi pe paginile web ale Serviciului Management Integrat IT. Se recomandă ca acest document să fie disponibil sau să se facă trimitere la acesta de pe toate sit- urile web din cadrul Universităţii din Oradea.

g) Modificarea prevederilor unui Regulament / Procedură se face cu aprobarea conducerii Universităţii din Oradea. Fiecare modificare a conţinutului va conduce la modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.

h) Conţinutul prezentului regulament este completat cu:

1. Anexa 1. Formular pentru alocarea de adresa de e-mail

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ

Anexa nr. 1

Formular pentru alocarea de adresa de e-mail

(1) Date de identificare:

Nume :

Prenume:

Fucţia:

Facultatea:

Departament:

Telefon birou: Email alternativ:

☐ Cadru didactic ☐ Angajat ☐ Doctorand ☑ Altele

(2) Aprobare sef superior:

Nume prenume Semnatura:

(3) Date referitoare la adresa de e-mail:

Nume utilizator propus:

Nume utilizator alocat:

Parola (acordată de administratorul de sitem):

Subsemnatul(a), **declar ca voi respecta** "Politica de securitate a Universităţii din Oradea" şi voi ţine cont de **recomandările făcute**.

Data:

Oradea

Semnătura

X

APROBAT ÎN ŞEDINŢA DE SENAT
DIN DATA DE
29. SEP. 2022
Preşedinte:
Conf.univ.dr. Vasile-Aurel CĂUŞ