ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
Nr. 3406
16 10 2023

APROB
PREȘEDINTE Filiala Cluj-Napoca

Doru PAMFIL

PROCEDURA OPERAŢIONALĂ
privind privind regulile de acces la reţeaua de comunicaţii
COD: PO–CIT-05

Ediția I, Revizia 0, Data 26.09.2023

Avizat
Președinte Comisiei de Sistem de Control Managerial Intern

Lucian CUIBUS

Verificat,
[Nume și prenume conducător compartiment/institut]
[Data și semnătura]

Elaborat,
Adrian COVACIU
Inspector de specialitate

1. CUPRINS

2. SCOPUL PROCEDURII

Acestea au ca scop principal protejarea utilizatorilor SI-ARFC împotriva atacurilor informatice de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii Academiei Române şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic.

Scopul acestei proceduri este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea sistemului informatic al ARFC în vederea îndeplinirii misiunii şi a obiectivelor instituţionale şi individuale;
- Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Compartimentul IT/ Responsabilul IT/ IIT;
- Şefii entităţilor organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale ARFCN. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către Responsabilul IT;
- Protejarea imaginii Academiei Române Filila Cluj;
- Protejarea investiţiilor Academiei Române Filila Cluj pentru dezvoltarea sistemului informatic;
- •Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Sistemul Informatic a utilizatorilor autorizaţi: personal administrativ, cercetători, colaboratori etc.
- Educarea utilizatorilor sistemului informatic în ceea ce priveşte responsabilităţile asociate cu utilizarea acestuia;
- Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea sistemului informatic.

2.1. Stabileşte modul de realizare a regulilor de acces la reţeaua de comunicaţii.

2.2. Dă asigurări cu privire la existenţa documentaţiei adecvate derulării activităţii de protejarea utilizatorilor.

2.3. Asigură continuitatea activităţii, inclusiv în condiţii de fluctuaţie a personalului.

2.4. Sprijină auditul şi/sau alte organisme abilitate în acţiuni de auditare şi/sau control şi pe conducătorii ARFC în luarea deciziei.

3. DOMENIUL DE APLICARE

3.1 **Precizarea (definirea) activității la care se referă procedura operațională:** Procedura se referă la regulile de acces în sistemul informatic realizată de personalul din cadrul compartimentului IT stabilind totodată reguile, normele și măsuri le de siguranță și protecție a datelor și informații lor din sistemul informatic.

3.2 Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate de entitatea publică. Activitatea este relevantă ca importanță, fiind procedurată distinct în cadrul instituției.

3.3 Listarea principalelor activități de care depinde și/sau care depind de activitatea procedurată. De activitatea procedurată depind toate celelalte activități din cadrul instituției, datorită rolului pe care această activitate îl are în cadrul derulări i corecte și la timp a tuturor proceselor.

3.4 Listarea compartimentelor furnizoare de date și/sau beneficiare de rezultate ale activității procedurate:

3.4.1 Compartimente furnizare de date: *Toate structurile*

3.4.2 Compartimente furnizoare de rezultate: *Toate structurile*

3.4.3 Compartimente implicate în procesul activității: *Toate structurile*

4. DOCUMENTE DE REFERINȚĂ

4.1. Reglementări internaționale

- ISO 17799 – Standard al Organizației Internaționale de Standardizare (ISO) ce conține recomandări privitoare la securitatea digitală. http://www.iso17799software.com/what.htm;
- ISO/CEI 27001: 2013 – Standard al Organizației Internaționale de Standardizare (ISO) pentru Securitatea Informatiei; Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;
- ISO/CEI 27002: 2018 - Standard al Organizației Internaționale de Standardizare (ISO) pentru Securitatea Informatiei;
- Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;
- Regulamentul (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor - GDPR)
- Directiva (UE) 2016/680 referitoare la protecția datelor personale în cadrul activităților specifice desfășurate de autoritățile de aplicare a legii

4.2. Legislație primară

- Legea nr. 8/1996 privind dreptul de autor și drepturile conexe;
- Legea nr. 455 din 18 iulie 2001 privind semnătura electronică;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public;
- Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate;
- Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
- Legea 506/2004 (TI) - privind prelucrarea datelor cu caracter personal și

protecţia vieţii private în cadrul comunicaţiilor electronice;

- Ordonanţa de Guvern nr.124/2000 (TI) - pentru completarea cadrului juridic privind dreptul de autor şi drepturile conexe, prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio şi video, precum şi a programelor pentru calculator;
- Legea 213/2002 (TI) - privind aprobarea Ordonanţei Guvernului nr. 124/2000 pentru completarea cadrului juridic privind dreptul de autor şi drepturile conexe prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio şi video, precum şi a programelor pentru calculator;
- Legea nr. 135/2007, legea privind arhivarea documentelor în forma electronică;
- 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;
- Ordinul nr. 279/2012 privind aprobarea modelului-cadru al protocolului de cooperare în vederea schimbului de informații între Agenția Națională de Administrare Fiscală și autoritățile administrației publice locale – (Preluare politica biroului curat)
- Legea nr. 190 din 18 iulie 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)
- Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice
- OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice
- Ghidul de securitate informatică pentru funcţionarii publici, CERT-RO;

4.3. Legislaţie secundară

a. Statutul Academiei Române;
b. Legea nr. 752/2001 privind organizarea şi funcţionarea Academiei Române cu modificările şi completările ulterioare

4.4. Alte documente, inclusiv reglementări interne ale entităţii publice

a. Regulamentul Intern al Academiei Române Filiala Cluj-Napoca;
b. Regulamentul de Organizare şi Funcţionare al Academiei Române Filiala Cluj-Napoca;
c. PS – ARFC 00

5. DEFINIȚII ȘI ABREVIERI

a. Definiții ale termenilor specifici utilizati în activitatea reglementată de prezenta PO

Nr. crt.	Termenul*	Definiția și/sau, dacă este cazul, actul normativ care definește termenul
1.	***Cont***	O entitate specificată printr-un identificator și/sau parolă pentru accesul la sistemul de comunicație și/sa la o resursă de calcul.
2.	***Date cu caracter personal***	Orice informatii privind o persoana fizica identificata sau identificabila (persoana vizata); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
3	***Eveniment privind securitatea informației***	Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei rețele indicând o posibilă încălcare a politicii de securitate a informației, un eșec al mijloacelor de control sau o situație ignorată anterior dar care poate fi relevantă din punct de vedere al securității.
4	***Gazdă (Host)***	Un sistem care oferă servicii pentru un anumit număr de utilizatori.
5	***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 integrității și/sau confidențialității informației 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 informațiilor, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără știința sau intenția utilizatorului.
6	***Incident privind securitatea informației***	Unul sau o serie de evenimente privind securitatea informației nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operațiunilor de business și de amenințare a securității informației.
7	***Internet***	Sistem global care interconectează calculatoare și rețele de calculatoare. Acestea sunt deținute de mai multe organizații, agenții guvernamentale, societăți, instituții academice.
8	***Intranet***	Rețea privată destinată comunicațiilor și partajării informațiilor, care, ca și rețeaua Internet, folosește suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizați din cadrul unei organizații (instituții). În mod obișnuit, rețeaua Intranet a unei organizații este protejată printr-un sistem de protecție (firewall).
9	***Protecție informațională***	Acțiuni întreprinse în vederea afectării informațiilor și sistemelor informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii.

10	***Securitatea fizică***	Domeniul securităţii care prezintă atât măsuri pentru prevenire cât şi pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informaţii şi recomandări privind proiectarea infrastructurii pentru a opune rezistenţă la actele ostile.
11	***Securitatea informaţiei***	Set de măsuri tehnice şi organizatorice care au ca scop asigurarea păstrarea confidenţialităţii, integrităţii şi a disponibilităţii informaţiei.
12	***Semnătură electronică***	Atribut indispensabil al documentului electronic, obţinut în urma transformării criptografice a acestuia, cu utilizarea cheii private, conform prevederilor Legii nr. 455/2001 privind semnătura electronică, republicată.
13	***Server***	Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.
14	***Sistem informatic***	Set integral de componente pentru colectarea, stocarea, prelucrarea datelor şi informaţiilor pentru furnizarea lor, cunoştinţelor şi a produselor digitale. Componentele unui sistem informatic sunt hardware, software, telecomunicaţii, datele prelucrate, baze de date, resurse umane, precum şi proceduri. Sistemul informatic al ARFC cuprinde resursele informatice şi de comunicaţii ale ARFC.
15	***Stocarea Externă (Offsite)***	Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de sediul ARFC 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/locaţie securizată din ARFC din Cluj poate înlocui stocarea externă.
16	***Resurse informatice şi de comunicaţii***	Toate dispozitivele de tipărire/imprimare, dispozitive de afişare, medii de stocare a informaţiilor, şi toate activităţile asociate calculatorului care implică utilizarea Sistemului Informatic, dispozitiv capabil să recepţioneze e-mail, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: *mainframe*-uri, servere, calculatoare personale, laptop-uri, calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), smartphone-uri, pagere, sisteme de

* Se vor defini doar termenii specifici utilizaţi în PO, pentru ceilaltă se va face trimitere la PS-ARFC.00.

b. Abrevieri

Nr. crt.	Abreviere	Termenul abreviat
1	**A**	Aprobare
2	**Ah.**	Arhivare
3	**Ap.**	Aplicare
4	**ARFC**	Academia Română - Filiala Cluj-Napoca
5	**CFC**	Compartiment Financiar -Contabilitate
6	**CRU**	Compartiment Resurse Umane
7	**CSAL**	CompartimentSalarizare
8	**CTA**	Compartiment Tehnic Administrativ
9	**CIT**	Compartiment IT
	CGT	Compartiment Granturi
10	**BVC**	Buget de venituri si cheltuieli
11	**CAP**	Compartiment Achiziții Publice
12	**CAPI**	Compartimentul de Audit Public Intern
13	**CJ**	CompartimentJuridic
14	**CSECR**	Compartiment Secretariat
15	**CREG**	Compartiment Registratură
16	**CMSCIM**	Comisia de monitorizare a Sistemului de Control Intern Managerial
17	**CtȘ**	Contabil șef al ARFC
18	**DAdj.ARFC**	Director adjunct în cadrul ARFC
19	**DI-ARFC**	Directorul de institut/centru/colectiv de cercetare din cadrul ARFC
20	**DP**	Directorul de proiect
21	**E**	Elaborare
22	**F**	Formular
23	**IL**	Instrucțiune de lucru
24	**PARFC**	Președintele Filialei Cluj-Napoca a Academiei Române
25	**PCM**	Președintele Comisiei de Monitorizare
26	**PS**	Procedură de sistem
27	**PO**	Procedură operațională
28	**SCIM**	Sistem de Control Intern Managerial
29	**V**	Verificare
30	**ILIL**	Institutul de Lingvistică și Istorie Literară "Sextil Pușcariu"
31	**BARCJ**	Biblioteca Academiei Române – Filiala Cluj-Napoca
32	**IGB**	Institutul de Istorie "George Barițiu – Departamentul de Istorie
33	**DCSU**	Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane
34	**CST**	Centrul de Studii Transilvane
35	**IAFAR**	Arhiva de Folclor a Academiei Române
36	**IAIA**	Institutul de Arheologie și Istoria Artei
37	**CGC**	Colectivul de Geografie Cluj
38	**ICTP**	Institutul de Calcul „Tiberiu Popoviciu"
39	**OACJ**	Observatorul Astronomic Cluj
40	**ISER**	Institutul de Speologie "Emil Racoviță" – ColectivulCluj
41	**ICSUMS**	Institutul de Cercetări Socio-Umane din Tg. Mureș

6. DESCRIEREA PROCEDURII

✓ Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Compartimentul IT/ Responsabilul IT/ IIT;
✓ Șefii entităților organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale ARFCN. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către Responsabilul IT;
✓ Conectarea sistemelor de calcul care nu sunt proprietatea ARFCN se face numai cu aprobarea în scris a Compartimentul IT la recomandarea Institutelor sau departamentelor;
✓ Accesul de la distanţă la reţeaua ARFCN se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către ARFCN şi folosind protocoale aprobate de către IIT/Responsabilul IT;
✓ Utilizatorii din interiorul ARFCN nu se pot conecta la altă reţea;
✓ Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în niciun fel, pe nicio cale. Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv;
✓ Autorizarea tuturor conexiunilor se face la propunerea Institutelor/Centrelor/Colectivelor de către responsabilul IT;
✓ Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea responsabilului IT;
✓ Sistemele computerizate din afara ARFCN care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale ARFCN;
✓ 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 ARFCN nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua ARFCN;
✓ Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni;
✓ Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul IT/ Responsabilul IT;
✓ Serviciile de interconectare a reţelei ARFCN cu alte reţele sunt realizate exclusiv de către Compartimentul IT/ Responsabilul IT;
✓ Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Compartimetului IT.

6.1 . Compartimentul IT are la bază următoarele obiective:

- să nu permită utilizatoriilor să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni;

✓ să nu permită utilizatoriilor să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua ARFCN;

- să configureze corect toate SI şi laptopurile privind accesul de la distanţă prin reţeaua securizată de tip VPN;

6.2 Documente utilizate

Documentele utilizate în elaborarea prezentei proceduri sunt cele enumerate la pct.4.

6.3 Resurse necesare

- Computer;
- Imprimantă;
- Copiator;
- Consumabile (cerneală/toner) ;
- Hartie xerox;
- Dosare.

6.4 Modul de lucru.

Planificarea şi acţiunilor activităţii:

Operaţiuni le şi acţiuni le privind activitatea procedurată se vor derula de către toate compartimentele, conform instrucţiuni lor din prezenta procedură.

6.5 Derularea operaţiunilor şi acţiunilor activităţii:

1. Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului informatic al Academiei Române Filiala Cluj-Napoca.
2. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din sistemul informatic pentru care nu au autorizaţie sau consimţământ explicit.
3. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau sau orice informaţii similare utilizate în scopuri de autorizare şi identificare.
4. Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemului informatic. De exemplu, utilizatorii ARFC nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.

7. RESPONSABILITĂŢII

Coordonatorul IT are următoarele responsabilităţi şi competenţe:

a) creează condiţiile de aplicare a prezentei procedurii;
b) monitorizează nivelul de conectare a userilor precum şi modul de implementare privind securitate informaţională şi propune masuri de optimizare a acestora;
c) numeşte responsabili care să asigure elaborarea / modificarea şi gestionarea procedurilor specifice în cadrul serviciului;

Oficiul Juridic are următoarele responsabilităţi şi competenţe:

a) aduce la cunoştinţa conducerii compartimentelor apariţia / modificarea actelor care reglementează sau legiferează activităţile specifice;

Preşedintele ARFC are următoarele responsabilităţi şi competenţe:

a) avizează PS şi PO elaborate;
b) conciliază aspecte neclare în relaţia realizator – avizator şi ia decizia finală în cazul lipsei consensului dintre realizator – avizatori.

8. FORMULAR DE EVIDENȚA MODIFICĂRIILOR

Nr. crt.	Numărul și data ediției	Numărul și data reviziei	Nr. pag. unde s-a efectuat modificarea	Descrierea modificării	Semnătura conducătorului compartimentului
1					
2					
3					
4					