ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
NR. 3715
16 10 2023

**APROB**
**PREȘEDINTE Filiala Cluj-Napoca**

**Doru PAMFIL**

# PROCEDURA OPERAŢIONALĂ
## privind utilizarea permanentă a resurselor informatice și de comunicații
## COD: PO–CIT-03

***Ediția I, Revizla 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 accesul fizic la resursele informatice şi de comunicaţii precum şi accesul fizic la toate încăperile în care sunt instalate RIC. De asemenea acestea au ca scop protejarea imaginii Academiei Române şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic.

Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea sistemului informatic al ARFCN în vederea îndeplinirii misiunii şi a obiectivelor instituţionale şi individuale;
- 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 ARFCN;
- Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat;
- Protejarea imaginii Academiei Române Filila Cluj-Napoca;
- Protejarea investiţiilor Academiei Române Filila Cluj-Napoca 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 activităţii de protejarea utilizatorilor şi controlul acces a personalului ARFCN;

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 ARFCN în luarea deciziei.

## 3. DOMENIUL DE APLICARE

3.1 **Precizarea (definirea) activității la care se referă procedura operațională:** Procedura se referă la activitatea privind acesul fizic la resursele informatice și de comunicații de administrare a sistemului informatic, precum și de regulile de acces de personalul din cadrul ARFCN.

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 protecția vieții

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 informaţii între Agenţia Naţională de Administrare Fiscală şi autorităţile administraţiei 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 – ARFCN 00

## 5. DEFINIȚII ȘI ABREVIERI

### 5.1. 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 character 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*** | Acțiuni întreprinse în vederea afectării informațiilor și sistemelor |

| | | |
|---|---|---|
| | ***informațională*** | informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii. |
| 10 | ***Securitatea fizică*** | Domeniul securității care prezintă atât măsuri pentru prevenire cât și pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informații și recomandări privind proiectarea infrastructurii pentru a opune rezistență la actele ostile. |
| 11 | ***Securitatea informației*** | Set de măsuri tehnice și organizatorice care au ca scop asigurarea păstrarea confidențialității, integrității și a disponibilității informației. |
| 12 | ***Semnătură electronică*** | Atribut indispensabil al documentului electronic, obținut 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 același calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe același calculator mai pot rula și alte programe de tip client sau server. |
| 14 | ***Sistem informatic*** | Set integral de componente pentru colectarea, stocarea, prelucrarea datelor și informațiilor pentru furnizarea lor, cunoștințelor și a produselor digitale. Componentele unui sistem informatic sunt hardware, software, telecomunicații, datele prelucrate, baze de date, resurse umane, precum și proceduri. Sistemul informatic al ARFCN cuprinde resursele informatice și de comunicații ale ARFCN. |
| 15 | ***Stocarea Externă (Offsite)*** | Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de sediul ARFCN în care este puțin probabil să se producă efecte de același tip în cazul unui dezastru. Pe baza unei evaluări a informației pentru care s-au realizat copii de siguranță, mutarea mediilor de backup din clădire și depozitarea lor într-o altă zonă/locație securizată din ARFCN poate înlocui stocarea externă. |
| 16 | ***Resurse informatice și de comunicații*** | Toate dispozitivele de tipărire/imprimare, dispozitive de afișare, medii de stocare a informațiilor, și toate activitățile asociate calculatorului care implică utilizarea Sistemului Informatic, dispozitiv capabil să recepționeze 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 utilizați în PO, pentru ceilalță se va face trimitere la PS-ARFCN.00.

## 5.2. Abrevieri

| Nr. crt. | Abreviere | Termenul abreviat |
|---|---|---|
| 1 | **A** | Aprobare |
| 2 | **Ah.** | Arhivare |
| 3 | **Ap.** | Aplicare |
| 4 | **ARFCN** | 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 |
| 10 | **CGT** | Compartiment Granturi |
| 11 | **BVC** | Buget de venituri si cheltuieli |
| 12 | **CAP** | Compartiment Achiziții Publice |
| 13 | **CAPI** | Compartimentul de Audit Public Intern |
| 14 | **CJ** | CompartimentJuridic |
| 15 | **CSECR** | Compartiment Secretariat |
| 16 | **CREG** | Compartiment Registratură |
| 17 | **CMSCIM** | Comisia de monitorizare a Sistemului de Control Intern Managerial |
| 18 | **CtȘ** | Contabil șef al ARFCN |
| 19 | **DAdj.ARFCN** | Director adjunct în cadrul ARFCN |
| 20 | **DI-ARFCN** | Directorul de institut/centru/colectiv de cercetare din cadrul ARFCN |
| 21 | **DP** | Directorul de proiect |
| 22 | **E** | Elaborare |
| 23 | **F** | Formular |
| 24 | **IL** | Instrucțiune de lucru |
| 25 | **PARFCN** | Președintele Filialei Cluj-Napoca a Academiei Române |
| 26 | **PCM** | Președintele Comisiei de Monitorizare |
| 27 | **PS** | Procedură de sistem |
| 28 | **PO** | Procedură operațională |
| 29 | **SCIM** | Sistem de Control Intern Managerial |
| 30 | **V** | Verificare |
| 31 | **ILIL** | Institutul de Lingvistică și Istorie Literară "Sextil Pușcariu" |
| 32 | **BARCJ** | Biblioteca Academiei Române – Filiala Cluj-Napoca |
| 33 | **IGB** | Institutul de Istorie "George Barițiu – Departamentul de Istorie |
| 34 | **DCSU** | Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane |
| 35 | **CST** | Centrul de Studii Transilvane |
| 36 | **IAFAR** | Arhiva de Folclor a Academiei Române |
| 37 | **IAIA** | Institutul de Arheologie și Istoria Artei |
| 38 | **CGC** | Colectivul de Geografie Cluj |
| 39 | **ICTP** | Institutul de Calcul „Tiberiu Popoviciu" |
| 40 | **OACJ** | Observatorul Astronomic Cluj |
| 41 | **ISER** | Institutul de Speologie "Emil Racoviță" – ColectivulCluj |
| 42 | **ICSUMS** | Institutul de Cercetări Socio-Umane din Tg. Mureș |

## 6. DESCRIEREA PROCEDURII

**Generalități**

6.1. Un sistem informatic este un sistem care permite introducerea de date prin procedee manuale sau prin culegere automată de către sistem, stocarea acestora, prelucrarea lor și extragerea informației (rezultatelor) sub diverse forme. Componentele sistemului informatic sunt: calculatoarele, programele, rețelele de calculatoare și utilizatorii.

6.2. Sistemul informatic conferă utilizatori lor următoarele avantaje:

- îmbunătățirea preciziei rezultatelor prelucrări lor, prin eliminarea erorilor umane care pot apărea într- un sistem manual de prelucrare și de procesare uniformă a datelor, pe măsura apariției acestora;
- creșterea vitezei de procesare, prin prelucrarea automată a datelor și el iminarea timpi lor de prelucrare manuală a acestora, oferind utilizatori lor informații solicitate, în momentul când aceștia au nevoie de ele;
- posibitatea salvării datelor cu ajutorul unități lor de stocare în cazul apariției unor defecte hardware, erori software, virusarea programelor care pot determina pierderea datelor.

6.3. Buna funcționare a sistemului informatic asigură realizarea următoarelor obiective:

- Asigurarea bunei funcționări și a reparațiilor componentelor sau calculatoarelor din dotarea instituției, care nu se mai află în garanție la firmele producătoare;
- Asigurarea asistenței tehnice de specialitate pentru achizițiile de echipamente IT noi, care să corespundă cerințelor echipamentelor existente și achiziției de calculatoare noi, conforme cu cerințele specifice ale instituției publ ice și Ia nivelul de performanță din momentul achiziției ;
- Asigurarea verificări lor periodice și întreținerea în stare de funcționare a tuturor echipamentelor din dotarea instituției;
- Asigurarea asistenței de specialitate, în măsura competențelor operatori lor IT cu privire Ia produsele software existente și executate de firme sau persoane autorizate care nu lucrează în instituție sau, în caz contrar, raportează erori le constatate;
- Asigurarea asistenței utilizatorilor în utilizarea diferitelor softwares;
- Asigurarea asistenței în implementarea noi lor produse software și asigurarea legăturii cu firmele producătoare sau cu persoanele de contact de la aceste firme;
- Analizarea, proiectarea și dezvoltarea de aplicații personalizate diferitelor procese desfășurate în activități le specifice în administrația publică;
- Monitorizarea software-ului specific serverelor de telecomunicații și de baze de date;
- Gestionarea conturi lor de utilizator pentru accesarea aplicațiilor financiar-contabile pentru personalul din instituția publică;
- Asigurarea funcționării, dezvoltării, depanării rețelei de calculatoare existente și a tuturor echipamentelor specific.

6.4. În vederea asigurării unui control intern eficient în sistemul de prelucrare a datelor utilizate de acestea se organizează controale organizatorice, ca metode și tehnici de organizare a activități lor desfășurate de instituție, folosite pentru prevenirea pierderi lor și/sau alterări lor de date determinate de fraudă, neatenție și/sau neglijență.

- în asigurarea controlului oricărui tip de sistem de prelucrare și evidentă a datelor este definirea clară a funcțiilor, urmată de definirea și separarea locală a sarcini lor și

responsabilităţi lor angajaţi lor pentru fiecare funcţie, nici un angajat nu trebuie să aibă sarcina şi răspunderea completă pentru efectuarea unei activităţi;

- operaţia executată de o persoană trebuie verificată de o altă persoană;
- pentru asigurarea bunei activităţi a sistemului informatic, administratorul de sistem are dreptul de a bloca accesul pe staţiile de lucru al persoanelor ce nu deţin anumite drepturi;
- utilizatorii îşi desfăşoară activitatea prin programele puse la dispoziţie de membrii compartimentului IT, utilizând user şi parola, acest lucru evidenţiindu-se în reţea, iar accesul la internet a fiecărei staţii de lucru este monitorizată în reţeaua de calculatoare prin alocarea unei adrese IP.

6.5 . Compartimentul IT are la bază următoarele obiective:

- Asigurarea depanării calculatoarelor, în măsura competenţelor, la calculatoarele care nu se află în termen de garanţie cu recuperarea echipamentelor, în scopul reducerii cheltuielilor de exploatare şi întreţinere;
- Asigurarea asistenţei tehnice de specialitate pentru achiziţiile de echipamente IT noi;
- Verificarea calităţii şi stării tehnice a echipamentelor IT cumpărate în cadrul licitaţiilor;
- Asigurarea verificărilor periodice şi întreţinerea în stare de funcţionare a tuturor calculatoarelor şi echipamentelor din instituţia publică;
- Asigurarea asistenţei, în măsura competenţelor, în ceea ce privesc produsele software existente şi executate de alte firme sau persoane autorizate din afara instituţiei; în caz contrar contactează personalul de conducere şi raportează erori le existente;
- Asigurarea asistenţei utilizatorilor în folosirea diferitelor produse software pentru a corespunde cerinţelor proiectate;
- Întreţinerea şi repararea softului specific serverelor de comunicaţii şi de baze de date;
- Gestionarea conturi lor de utilizator pentru accesarea internetului şi a conturi lor de e-mail pentru personalul din cadrul instituţiei;
- Asigurarea funcţionării, dezvoltării şi depanării reţelei de calculatoare şi a tuturor echipamentelor specifice;
- Întocmirea Notei de fundamentare privind realizarea Planului anual de investiţii pentru echipamentele de calcul şi extinderea reţelelor, necesare aducerii la parametrii optimi, în funcţie de modificări le organizatorice şi de personal din cadrul instituţiei publice.

6.6 **Documente utilizate**

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

6.7 **Resurse necesare**

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

6.8 **Modul de lucru**

**Planificarea operațiunilor și acțiunilor activității:**

Operațiuni le și acțiuni le privind activitatea procedurată se vor derula de către toate compartimentele, conform instrucțiuni lor din prezenta procedură.

**Derularea operațiunilor și acțiunilor activității:**

1. Utilizarea Resurselor Informatice și de Comunicații ARFCN se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunțe șeful ierarhic, RSSI și DPO în cazul în care se observă orice problemă/breșă în sistemul de securitate a sistemului informatic din cadrul Academiei Române Filiala Cluj-Napoca cât și orice posibilă întrebuințare greșită sau încălcare a regulamentelor în vigoare.
3. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul sistemului informatic al Academiei Române Filiala Cluj-Napoca.
4. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din sistemul informatic pentru care nu au autorizație sau consimțământ explicit.
5. 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 și/sau sau orice informații similare utilizate în scopuri de autorizare și identificare.
6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea Compartimentului IT/ Responsabilului IT, cu excepția cazului în care acestea se găsesc incluse în lista programelor de tip shareware sau freeware utilizate în cadrul ARFCN (Anexa nr. 23 Lista programelor de tip shareware sau freeware) sau în lista programelor standard folosite în cadrul ARFCN (Anexa nr. 24 - Lista aplicațiilor software permise a fi folosite în cadrul Academiei Române Filiala Cluj-Napoca). Actualizarea acestor liste va fi realizată de către Compartimentul IT la propunerea responsabililor IT din cadrul Institutelor /Centrelor /Departamentelor ARFCN.
8. Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane;
9. Să degradeze performanțele sistemului informatic; să împiedice accesul unui utilizator autorizat la sistemul informatic;
10. Să obțină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.
11. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemului informatic. De exemplu, utilizatorii ARFCN nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
12. Sistemul informatic al Academiei Române Filiala Cluj **NU trebuie folosit pentru beneficiul personal.** Se interzice scoaterea informației sau echipamentelor din sediul ARFCN fără autorizarea/aprobarea șefului ierarhic și/sau a conducerii ARFCN. În situația în care este necesară scoaterea informației sau echipamentelor din sediu, se va face o solicitare scrisă prin care se va motiva/justifica necesitatea scoaterii informației sau a echipamentelor.

13. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care ARFCN 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 ARFCN).

14. Accesul la rețeaua Internet prin intermediul sistemului informatic ARFCN se supune acelorași regulamente care se aplică utilizării din interiorul instituției și Regulamentului pentru Utilizare Internet și Intranet.

15. Angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la sistemului informatic al Academiei Române Filiala Cluj-Napoca.

16. Utilizatorii care au acces la sistemul informatic al Academiei Române Filiala Cluj-Napoca au obligația de a purta acte și/sau legitimații de serviciu care să ateste calitatea de utilizator autorizat în spațiile ARFCN.

17. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Academiei Române Filiala Cluj-Napoca folosind resursele sistemului informatic.

18. Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Academiei Române Filiala Cluj-Napoca sau prejudicierea, indiferent de formă, a intereselor ARFCN .

19. Toate stațiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului (Lock prin apăsarea simultană a tastei Windows și a tastei "L"), log off sau cu un screensaver protejat cu parolă, cu funcția de activare automată setată la 5 minute sau mai puțin. La sfârșitul programului de lucru acestea, precum și orice aparatură electrică și electronică, trebuie să fie oprite.

20. CD-urile, DVD-urile și alte medii de stocare nu trebuiesc lăsate la vedere atunci când nu sunt folosite. Daca ele conțin date de maximă confidențialitate, trebuie să fie ținute sub cheie. CD-urile, DVD-urile, mediile de stocare mobile trebuie păstrate departe de acțiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui și câmpuri magnetice.

21. Toate mesajele, fișierele și documentele localizate în cadrul SI-ARFCN sunt proprietatea Filialei și pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

## 7. RESPONSABILITĂȚII

**Coordonatorul IT are următoarele responsabilități și competențe:**

a) creează condițiile de aplicare a prezentei procedurii;
b) monitorizează nivelul de securitate informațională și propune masuri de optimizare;
c) numește responsabili care să asigure elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;

**Oficiul Juridic are următoarele responsabilități și competențe:**

a) aduce la cunoștința conducerii compartimentelor apariția / modificarea actelor care reglementează sau legiferează activitățile specifice;

**Președintele ARFCN are următoarele responsabilități și competențe:**

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