ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
Nr. 3713 /
16 10 2023

**APROB**

**PREȘEDINTE Filiala Cluj-Napoca**

**Doru PAMFIL**

# PROCEDURA OPERAŢIONALĂ

## privind securitatea informațiilor și a sistemului IT

## COD: PO–CIT-01

***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*

Cuprins

## 1. SCOPUL PROCEDURII

Procedura stabileşte politicile, principiile şi modalităţile de acţiune pentru asigurării securităţii informaţiilor şi a sistemului IT din cadrul ARFCN.

## 2. DOMENIUL DE APLICARE

Procedura se aplică în toate Institutele / Centrele/ Colectivele ARFCN şi toate compartimentele aferente ARFCN

## 3. DOCUMENTE DE REFERINŢĂ

### 3.1. Reglementări internaţionale

3.3.1 RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
3.3.2 ISO 17799 – Standard detaliat de securitate https://www.iso.org/standard/46381.html
3.3.3 Convenţia privind criminalitatea informatică - Monitorul Oficial, Partea I nr. 343 din 20/04/2004
3.3.4 Declaraţia privind libertatea comunicării pe Internet adoptată la Strasbourg în 2003

### 3.2. Legislaţie primară

3.2.1 Legea nr. 8/1996 - privind dreptul de autor şi drepturile conexe, cu modificările şi completările ulterioare
3.2.2 Lege nr. 455/2001 - privind semnătura electronică, cu modificările şi completările ulterioare
3.2.3 Lege nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulatie a acestor date, cu modificările şi completările ulterioare
3.2.4 HG nr. 1007/2001 - privind aprobarea strategiei guvernului privind informatizarea administraţiei publice
3.2.5 Legea 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare;

### 3.3. Legislaţie secundară

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

### *3.4. 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

## 4. DEFINIȚII ȘI ABREVIERI

### 4.1 Termeni și definiții

4.1.1 **Virus informatic** - Un program care se atașează la un fișier executabil sau la o aplicație vulnerabilă și care generează efecte deranjante sau distructive. Un virus se execută în momentul în care este accesat un fișier infectat.

4.1.2 **Vierme** - Un program care se auto-copiază în spațiul de stocare al unui sistem informatic și care se răspândește către alte calculatoare prin intermediul rețelei. Unii dintre acești viermi reprezintă o amenințare la adresa securității informatice datorită faptului că folosesc rețeaua pentru a se multiplica, determinând nefuncționarea sau funcționarea defectuoasă a rețelei.

4.1.3 Cal troian – Este obicei un virus sau un vierme care este disimulat sub forma unui program atractiv sau inofensiv. Acesta se poate răspândi prin email, prin utilizarea un stick de memorie sau prin descarcarea din retea a unor fisiere compromise.

4.1.4 **Phishing** – un atac de *phising* are loc atunci când se încearcă inducerea în eroare a unui utilizator astfel încât acesta să furnizeze online informații de identificare sau cu caracter personal. De obicei, *phishing*-ul are loc prin e-mail sau prin site-uri care arată similar cu site-uri cunoscute.

4.1.5 **Ransoms** – este un *malware* care blochează computerul sau criptează fișierele. De obicei pentru deblocarea sistemului și/sau recuperarea fișierelor se solicită plați în scopul declarat de furnizare ulterioara a cheilor de decriptare, neexistând însă nicio garanție că datele vor fi recuperate în acest mod.

4.1.6 **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.

4.1.7 **Expunere** - Reducerea a constrângerilor impuse pentru accesarea informațiilor.

4.1.8 **Vulnerabilitate** - Slăbiciune care poate fi exploatată în scopul accesării neautorizate a resurselor sau informațiilor.

4.1.9 **Atac** - Încercarea de a exploata vulnerabilitatea.

4.1.10 **Control** - Măsură de gestionare vulnerabilității de obicei in scopul reducerii expunerii la riscuri.

| Nr. crt. | Termenul* | Definiţia şi/sau, dacă este cazul, actul normativ care defineşte termenul |
|---|---|---|
| 1. | ***Cont*** | O entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/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 informaţiei*** | Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei reţele indicând o posibilă încălcare a politicii de securitate a informaţiei, un eşec al mijloacelor de control sau o situaţie ignorată anterior dar care poate fi relevantă din punct de vedere al securităţii. |
| 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 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. |
| 6 | ***Incident privind securitatea informaţiei*** | Unul sau o serie de evenimente privind securitatea informaţiei nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operaţiunilor de business şi de ameninţare a securităţii informaţiei. |
| 7 | ***Internet*** | Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, |

| | | |
|---|---|---|
| | | agenţii guvernamentale, societăţi, instituţii academice. |
| 8 | ***Intranet*** | 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). |
| 9 | ***Protecţie informaţională*** | Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi 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 | | Toate dispozitivele de tipărire/imprimare, dispozitive de afişare, medii de stocare a informaţiilor, şi toate activităţile asociate calculatorului care implică utilizarea Sistemului Informatic, |

| | | |
|---|---|---|
| | ***Resurse informatice și de comunicații*** | 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-ARFC.00.

**a. 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** | Compartiment Salarizare |
| 8 | **CTA** | Compartiment Tehnic Administrativ |
| 9 | **CIT** | Compartiment IT |
| 10 | **CGT** | Compartiment Granturi |
| 11 | **CSSM** | Compartiment Securitate și Sănătate în Muncă |
| 12 | **BVC** | Buget de venituri si cheltuieli |
| 13 | **CAP** | Compartiment Achiziții Publice |
| 14 | **CAPI** | Compartimentul de Audit Public Intern |
| 15 | **CJ** | Compartiment Juridic |
| 16 | **CSECR** | Compartiment Secretariat |
| 17 | **CREG** | Compartiment Registratură |
| 18 | **CPA** | Compartiment Patrimoniu |
| 19 | **CRP** | Compartiment Relații Publice |

| | | |
|---|---|---|
| 18 | **CMSCIM** | Comisia de monitorizare a Sistemului de Control Intern Managerial |
| 19 | **CTŞ** | Contabil şef al ARFCN |
| 20 | **DAdj.ARFCN** | Director adjunct în cadrul ARFCN |
| 21 | **DI-ARFCN** | Directorul de institut/centru/colectiv de cercetare din cadrul ARFCN |
| 22 | **DP** | Directorul de proiect |
| 23 | **E** | Elaborare |
| 24 | **F** | Formular |
| 25 | **IL** | Instrucțiune de lucru |
| 26 | **PARFCN** | Preşedintele Filialei Cluj-Napoca a Academiei Române |
| 27 | **PCM** | Preşedintele Comisiei de Monitorizare |
| 28 | **PS** | Procedură de sistem |
| 29 | **PO** | Procedură operațională |
| 30 | **SCIM** | Sistem de Control Intern Managerial |
| 31 | **V** | Verificare |
| 32 | **ILIL** | Institutul de Lingvistică și Istorie Literară "Sextil Pușcariu" |
| 33 | **BARCJ** | Biblioteca Academiei Române – Filiala Cluj-Napoca |
| 34 | **IGB** | Institutul de Istorie "George Barițiu – Departamentul de Istorie |
| 35 | **DCSU** | Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane |
| 36 | **CST** | Centrul de Studii Transilvane |
| 37 | **IAFAR** | Arhiva de Folclor a Academiei Române |
| 38 | **IAIA** | Institutul de Arheologie și Istoria Artei |
| 39 | **CGC** | Colectivul de Geografie Cluj |
| 40 | **ICTP** | Institutul de Calcul „Tiberiu Popoviciu" |
| 41 | **OACJ** | Observatorul Astronomic Cluj |
| 42 | **ISER** | Institutul de Speologie "Emil Racoviță" – ColectivulCluj |
| 43 | **ICSUMS** | Institutul de Cercetări Socio-Umane din Tg. Mureș |

## 5. CONȚINUT

### 5.1 Principiile asigurării securității informaționale

5.1.1 Principiile care trebuie îndeplinite pentru a asigura securitatea sistemelor informatice sunt:

a) **Principiul responsabilității.** Responsabilitățile legate de securitate informațională pentru deținători, furnizori și utilizatori de sisteme informatice sau servicii de date trebuie să fie explicite.

b) **Principiul conștientizării.** Pentru a asigura securitatea sistemelor informatice, deținătorii, furnizorii și utilizatorii acestora trebuie să poată accesa și dobândi cunoștințele necesare, să fie informați despre existența și cadrul general al măsurilor, practicilor și procedurilor de securitate a sistemelor informatice și să poată acționa voluntar pentru reducerea riscurilor.

c) **Principiul eticii.** Sistemele informatice și securitatea sistemelor informatice trebuie folosite într-o manieră în care drepturile și interesele legale ale celorlalți să nu fie afectate.

d) **Principiul multidisciplinarității.** Măsurile, practicile și procedurile de asigurare a securității sistemelor informatice trebuie să țină cont de toate considerațiile și aspectele relevante, inclusiv tehnice, administrative, organizaționale, operaționale, comerciale, educaționale și legale.

e) **Principiul proporționalității.** Nivelurile de securitate, costurile, măsurile, practicile și procedurile trebuie să fie corespunzător dimensionate și proporționale cu valoarea și gradul de încredere necesar pentru fiecare tip de informație avându-se în vedere de asemenea și nivelul daunelor potențiale respectiv probabilitatea de apariție a acestora.

f) **Principiul integrării.** Măsurile, practicile și procedeele de asigurare a securității sistemelor informatice trebuie să fie coordonate instituțional și integrate și cu alte măsuri, practici și procedee ale organizației cu scopul creării unui sistem global de securitate informațională coerent.

g) **Principiul actualității.** Instituțiile, indiferent de tipul lor, trebuie să acționeze rapid și într-o manieră coordonată pentru a preveni și a răspunde eficient la apariția breșelor de securitate a sistemelor informatice.

h) **Principiul reevaluării.** Securitatea sistemelor informatice trebuie analizată și reevaluată periodic pentru a răspunde celor mai noi tipuri de agresiuni informatice.

i) **Principiul democrației.** Securitatea sistemelor informatice trebuie să nu restrângă drepturile de utilizare legitimă a rețelelor de date.

5.1.2 Politica de securitate a resurselor informatice are ca scop asigurarea integrității, confidențialității și disponibilității informației.

a) *Confidențialitatea* se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul ARFCN, sunt proprietatea instituției în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la resursele informatice.

b) *Integritatea* se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

c) *Disponibilitatea* se asigură prin funcţionarea continuă a tuturor componentelor sistemului şi resurselor informatice. Aplicaţiile informatice au nevoie de niveluri diferite de disponibilitate în funcţie de impactul sau daunele ce pot fi produse ca urmare a nefuncţionării lor corespunzătoare. Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii resurselor informatice.

## 5.2 Politica de securitate în utilizarea resurselor informatice din cadrul ARFCN

5.2.1 Scopul elaborării politicii de securitate informaţională

a) Politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate;
b) Politica de securitate este implementată prin reguli şi măsuri menite să asigure securitatea informaţiilor specifice instituţiei;
c) reglementările rezultate din politica de securitate sunt obligatorii pentru toţi utilizatorii resurselor informatice.

5.2.2 La întocmirea planului asigurare a securităţii informaţionale a reţelei IT se au în vedere tipurile posibile de ameninţări şi/sau acţiuni:

a) **Forţa majoră**: pierderea personalului; inundaţie; incendiu;
b) **Deficienţe de organizare**: utilizarea incorectă sau neadecvată a resurselor IT; folosirea neautorizată a drepturilor de utilizare;
c) **Greşeli umane**: distrugerea din neglijenţă a unor echipamente sau a unor date; nerespectarea măsurilor de securitate; defecţiuni datorate acţiunilor improprii ale personalului de întreţinere sau intervenţie; administrarea necorespunzătoare a sistemului de securitate implementat; organizarea defectuoasă a gestionării informaţiilor şi datelor;
d) **Defecţiuni tehnice**: indisponibilitatea surselor de alimentare cu energie electrică; parametri improprii ai energiei electrice; nefuncţionarea sisteme de stocare/ înregistrare a datelor; existenţa unor vulnerabilităţi ale programelor folosite; acces impropriu la mecanismul tehnic de gestiune a securităţii informaţionale;
e) **Acte deliberate**: manipularea sau distrugerea echipamentului de protecţie a reţelei sau a accesoriilor sale; manipularea frauduloasa a datelor sau a programelor informatice; furt; interceptarea canalelor şi liniilor de date ale infrastructurii; accesarea si/sau modificarea neautorizată a sistemului de protecţie al reţelei; încercarea sistematică de descoperire a parolelor de acces; utilizarea abuzivă a drepturilor de utilizator; limitarea sau blocarea drepturilor de administrare; facilitarea pătrunderii de viruşi/troieni informatici în reţea; furtul de identitate şi accesarea astfel a unor drepturi pentru care nu există autorizare; urmărirea traficului de date; blocarea prin diverse metode a unor servicii sau porturi de date.

5.2.3 Reguli de utilizare corectă a resurselor informatice

a) Utilizatorii trebuie să anunţe SCTI în cazul în care se observă orice problemă sau breşă în sistemul de securitate al ARFCN cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentului în vigoare.
b) 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 din sistem.

c) Utilizatorii nu trebuie să încerce să obţină acces la date sau programe pentru care nu au autorizaţie sau consimţământ explicit.

d) Utilizatorii nu trebuie să divulge sau să înstrăineze datele de autentificare proprii (nume de cont-uri, parole etc.) utilizate în scopuri de autorizare şi identificare în reţeaua informaţională a instituţiei.

e) Utilizatorilor nu le este permis să realizeze copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).

f) Se recomandă ca utilizarea de programe de tip *shareware* sau *freeware* sa se faca cu responsabilitate, eventual cu consultarea responsabilului de domeniu dacă se consideră necesar.

g) Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de penetrare a unor restricţii de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemului informatic al instituţiei.

h) Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care instituţia le poate considera ofensive, indecente sau obscene.

i) Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor ARFCN folosind resursele informatice.

5.2.4 Accesul fizic: toate încăperile în care sunt instalate echipamente ale sistemului informatic trebuie să fie protejate la accesarea fizică neautorizată, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.

5.2.5 Confidenţialitatea serviciilor informatice

a) În scopul administrării sistemului informatic şi pentru asigurarea securităţii acestuia personalul autorizat poate monitoriza activitatea din reţeaua de date cu respectarea confidenţialităţii, în conformitate cu legile în vigoare.

b) Utilizatorii trebuie să informeze responsabilul IT în legătură cu eventualele suspiciuni de încălcare a confidenţialităţii şi să ofere, dacă este posibil, informaţiile necesare pentru identificarea problemei.

c) Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicare ale terţilor nu poate fi asigurată implicit. Pentru astfel de situaţii, asigurarea confidenţialităţii şi integrităţii informaţiilor sensibile este o obligaţie a utilizatorilor şi are la baza folosirea tehnicilor de securizare (criptare, conexiuni VPN).

5.2.6 Configurarea parametrilor de acces la reţea

a) Reţeaua informatică a ARFCN este administrată de către compartimentul IT care este responsabil cu întreţinerea şi dezvoltarea acesteia.

b) Toate echipamentele conectate la reţea vor fi configurate conform specificaţiilor IT

c) Reţeaua locală ARFCN este de tip Ethernet si suportă un set de protocoale de comunicaţie de reţea în conformitate cu scopul şi misiunea instituţiei.

d) Adresele de reţea sunt gestionate centralizat exclusiv de către responsabilul IT

e) Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei ARFCN; este interzisă instalarea de echipamente (*router*, *switch*, *hub* sau punct de acces) în reţeaua Intranet ARFCN fără avizul responsabilul IT.

5.2.7 Monitorizarea resurselor informatice

a) Monitorizarea reţelei se va face astfel încât să fie posibilă detectarea în timp util a

atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate.

b) Fişierele jurnal vor fi stocate şi vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale instituţiei. În această categorie intră următoarele (fără a se limita doar la acestea):
   1. Jurnale ale activităţii conturilor utilizator;
   2. Jurnale ale scanărilor reţea;
   3. Jurnale ale aplicaţiilor;
   4. Jurnale ale solicitărilor de suport tehnic;
   5. Jurnale ale erorilor din sisteme şi servere.

5.2.8 Securitatea serverelor

a) Un server nu trebuie conectat la reţeaua instituţiei decât atunci când este securizat adecvat.

b) Procedura de securizare a serverelor include obligatoriu următoarele:
   1. instalarea sistemului de operare dintr-o sursă veridică, aprobată;
   2. aplicarea *patch*-urilor furnizate de producător;
   3. înlăturarea programelor, a serviciilor sistem şi a driverelor care nu sunt necesare;
   4. setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
   5. dezactivarea sau schimbarea parolelor predefinite;
   6. securizarea accesului la servicii din Internet;
   7. securizarea accesului fizic la echipamente.

5.2.9 Parole de acces

a) Toate parolele trebuie să îndeplinească următoarele condiţii:
   1. Să fie schimbate de utilizator în mod regulat;
   2. Să aibă o lungime, un număr de caractere, cat mai mare;
   3. Să aba diversitate cat mai mare ca şi caractere utilizate;
   4. Reutilizarea parolelor este interzisă;
   5. Parolele stocate trebuie securizate;
   6. Parolele de cont utilizator nu trebuie divulgate către terţi sub nici o formă, fără excepţie;

b) Dacă se suspectează că o parolă a fost divulgată aceasta trebuie schimbată imediat;

c) Este recomandabil ca utilizatorii să nu folosească programe de stocare a parolelor;

d) Calculatoarele nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea pe bază de parolă;

e) Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

1. Utilizatorul se va legitima pe baza IP iar administratorul de sistem va verifica drepturile de acces ale persoanei la contul utilizator;
2. Se va genera o parolă care va fi comunicată utilizatorului;
3. Utilizatorul va schimba parola temporară, comunicată anterior, în cel mai scurt timp posibil.

5.2.10 Recomandări generale pentru alegerea parolelor:

a) Parolele trebuie să fie schimbate după cel mult 6 luni de utilizare;

b) Parolele trebuie să aibă o lungime minimă recomandată de 11 caractere;

c) Parolele trebuie să conţină o varietate cat mai mare de caractere (litere mici şi mari,

caractere numerice şi caractere speciale acolo unde sistemul permite).

d) Parolele trebuie să respecte următoarele condiţii:
   1. nu trebuie să coincidă sau să fie asemănătoare cu numele de utilizator (*login*-ul);
   2. nu trebuie să coincidă sau să fie asemănătoare cu numele utilizatorului;
   3. nu trebuie să coincidă cu date personale (codul numeric personal, data naşterii; numele străzii/oraşului; numărul de telefon etc.)
   4. parolele trebuie tratate ca informaţie confidenţială şi nu trebuie divulgate în nici o situaţie.

5.2.11 Sistemul de mesagerie electronică

a) Următoarele activităţi sunt interzise:
   1. trimiterea de mesaje cu caracter de intimidare sau hărţuire;
   2. folosirea sistemului de mesagerie electronică în alte scopuri decât cele profesionale;
   3. încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
   4. folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile în care persoana este autorizată administrativ în acest scop;
   5. folosirea programelor de poştă electronică neautorizate.

b) Următoarele activităţi asociate comunicaţiilor de grup sunt interzise deoarece împiedică buna funcţionare a reţelei şi reduce eficienţa comunicărilor electronice:
   1. trimiterea sau retrimiterea email-urilor în lanţ;
   2. trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
   3. trimiterea mesajelor de dimensiuni foarte mari;
   4. trimiterea sau retrimiterea mesajelor identificate ca fiind suspecte şi care ar putea conţine viruşi;

5.2.12 Instruire şi informare

a) Informarea angajaţilor poate fi făcută la angajare, periodic sau de câte ori este nevoie. Este importantă comunicarea modificărilor realizate în politicile de securitate, datorate eventualelor modificări legislative;

b) Instruirea angajaţilor cu privire la riscurile care conduc la o utilizare necorespunzătoare, intenţionată sau neintenţionată. Angajaţii trebuie să cunoască, care sunt ameninţările, cum pot fi eliminate riscurile, eventualele probleme legale generate de utilizările necorespunzătoare.

5.2.13 Monitorizare

a) activităţile utilizatorilor în cadrul reţelei de date şi care implică accesul şi/sau folosirea sistemului informatic al ARFCN pot fi înregistrate şi analizate.

b) înregistrările activităţilor de utilizare a sistemului informatic al ARFCN sunt folosite exclusiv în scopul identificării acţiunilor ilegale sau abuzive şi respectă criteriile de confidenţialitate instituţională şi personală.

## 5.3 Măsuri şi reguli pentru asigurarea securităţii sistemului informatic

5.3.1 Măsuri generale de securitate:

a) asigurarea alimentării sigure cu energie electrica folosind surse de alimentare neîntreruptibile;

b) realizarea de verificări şi revizii tehnice periodice;
c) interzicerea utilizării de programe neautorizate;
d) utilizarea de parole conforme şi schimbarea periodică a acestora;
e) identificarea permanentă a vulnerabilităţilor sistemelor de protecţie; verificarea periodică a nivelului de securitate a reţelei (audit de securitate informaţională);
f) educarea personalului în legătură cu măsurile de securitate necesare şi instruirea acestuia pentru utilizarea de programe specifice;
g) verificarea periodică a sistemelor cu ajutorul programelor anti-virus şi asigurarea actualizării permanente a listelor cu definiţiile viruşilor;
h) autentificarea în reţea trebuie asigurată numai prin conexiuni de date securizate;
i) gestiunea corecta a copiilor de rezervă (*back-up*) în ceea ce priveşte securitatea, integritatea şi disponibilitatea acestora prin verificarea permanentă a funcţionalităţii mediilor de păstrare a datelor şi a ne-alterării conţinutului;

5.3.2 Reguli de bază pentru utilizatorii individuali ai sistemelor din reţea:
a) utilizatorii reţelei trebuie să salveze periodic datele importante cu care lucrează (documente, imagini, baze de date, etc.) pe un suport extern; suportul extern se va deconecta de la calculator după ce se finalizează operaţiunea de copiere iar acesta va fi păstrat intr-un loc sigur;
b) utilizatorii pot solicita instruirea pentru folosirea în siguranţă a staţiei de lucru şi pentru deprinderea modalităţilor de salvare periodică a datelor de interes;
c) utilizatorii sistemelor vor urmări actualizarea periodică a sistemului de operare, a programului antivirus instalat precum şi actualizarea altor aplicaţii software utilizate, dacă este cazul;
d) utilizatorii nu vor instala pe staţiile pe care lucrează programe neautorizate, programe fără licenţă sau pentru care nu există drepturi legale de utilizare sau aplicaţii care nu au legătură cu activitatea profesională desfăşurată în cadrul instituţiei;
e) utilizatorii vor folosi pentru transmiterea/primirea de mesaje electronice de serviciu adresele email instituţionale definite în domeniul administrate de IT (ex: nume.prenume utilizator@ academia-cj.ro );
f) Se va evita pe cât posibil utilizarea memoriilor externe de tip *flash* (*stick* de date) pentru a reduce expunerea la viruşi informatici atât a staţiei proprii de lucru cât şi a reţelei ARFCN;
g) Atunci când este posibil utilizatorul va verifica credibilitatea sursei unui mesaj email şi va investiga formal autenticitatea acestuia evitând deschiderea fişierelor ataşate suspecte;

5.3.3 Utilizarea dispozitivelor conectate la reţea (rutere wireless, sisteme DVR, camere ip, echipamente de măsură, sisteme SmartTV, etc):
a) parolele implicite (*default*) de pe dispozitive vor fi înlocuite imediat ce este posibil;
b) *firmware*-ul dispozitivelor trebuie să fie permanent actualizat;
c) opţiunile de tip *remote management* trebuie să fie limitate la strictul necesar pentru administrare.

5.3.4 Reguli de securitate şi conectare la reţeaua wireless:
a) accesul wireless în reţeaua ARFCN se realizează in mod obişnuit prin autentificare;
b) în condiţii bine definite este posibil accesul public de tip *guest*

c) este recomandată evitarea utilizării conexiunilor ne-criptate;
d) *router-ele* instalate în spatiile ARFCN trebuie să fie configurate și securizate conform recomandărilor IT; este interzisă conectarea *router*-elor sau punctelor de acces fără avizul responsabilului IT;
e) *router-ele* și punctele de acces altele decât cele administrate de administratorul de rețea și destinate accesului public cu/fără autentificare vor fi definite (SSID) într-o manieră care sa permită identificarea acestora și a amplasamentului lor fizic (corp clădire, număr sală/birou);

5.3.5 Politica de securitate a dispozitivelor mobile (telefoane, tablete):
a) sistemul de operare și aplicațiile utilizate trebuie sa fie actualizate periodic;
b) se recomandă conectarea doar la *router-e wireless* securizate (cu parolă);
c) dispozitivele mobile nu vor avea alocate adrese IP fixe, alocarea acestora se face automat în rețeaua wireless ARFCN

### 5.4 Monitorizarea eficienței rețelei informatice

5.4.1 Protecția eficientă a rețelei informatice a instituției conduce la creșterea indicatorilor de performanță asociați utilizării acesteia și la îmbunătățirea gradului de satisfacție al beneficiarilor direcți.
Indicatori urmăriți:
a) eficiența accesului la resurse electronice de informare, comunicare electronică și transfer de date;
b) nivelul de performanță al echipamentelor de comunicație și al infrastructurii de date;
c) gradul de creștere a operativității îndeplinirii sarcinilor de către salariați;
d) gradul de diminuare a timpului necesar elaborării documentelor standard;
e) gradul de creștere a operativității în furnizarea de informații sau documente către solicitanți;
f) nivelul general de satisfacție al utilizatorilor rețelei de date ARFCN.

## 6. RESPONSABILITĂȚI

6.1 **Responsabilul 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) propune responsabili care să asigure elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;

6.2 **Oficiul Juridic** are următoarele responsabilități și competențe:
a) aduce la cunoștința conducerii compartimentelor apariția / modificarea actelor care reglementează sau legiferează activitățile specifice;

6.3 **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.

## 7. DISPOZIȚII FINALE

**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 | | | | | |

ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
NR. 3712
16 10 2023

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

**Doru PAMFIL**

# PROCEDURA OPERAŢIONALĂ

## privind utilizarea ocazională a resurselor Informatice şi de Comunicaţii

## COD: PO–CIT-02

***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

## 1. CUPRINS

## 2. SCOPUL PROCEDURII

Acestea au ca scop principal protejarea utilizatorilor SI-ARFCN 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 acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile privind utilizarea ocazională a resurselor în folosirea sistemului informatic al ARFCN în vederea îndeplinirii misiunii şi a obiectivelor instituţionale şi individuale;
- Protejarea imaginii Academiei Române Filila Cluj-Napoca;
- 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.

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 ARFCNîn luarea deciziei.

## 3. DOMENIUL DE APLICARE

3.1 **Precizarea (definirea) activităţii la care se referă procedura operaţională:** Procedura se referă la activitatea privind utilizarea ocazională a resurselor informatice şi de comunicaţii din cadrul ARFCN, stabilind totodată reguile, normele şi măsuri le de siguranţă şi protecţie a datelor şi informaţii lor din sistemul informatic.

3.2 Delimitarea explicită a activităţii procedurate în cadrul portofoliului de activităţi desfăşurate de entitatea publică: Activitatea este relevantă ca importanţă, fi ind procedurată distinct în cadrul instituţiei.

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

3.4 Listarea compartimentelor furnizoare de date şi/sau beneficiare de rezultate ale activităţii 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 activităţii: *Toate structurile*

## 4. DOCUMENTE DE REFERINŢĂ

### *4.1. Reglementări internaţionale*

- ISO 17799 – Standard al Organizaţiei Internaţionale de Standardizare (ISO) ce conţine recomandări privitoare la securitatea digitală. http://www.iso17799software.com/what.htm;
- ISO/CEI 27001: 2013 – Standard al Organizaţiei Internaţionale de Standardizare (ISO) pentru Securitatea Informatiei; Tehnologia informaţiei. Tehnici de securitate. Sisteme de management a securităţii informaţiei;
- ISO/CEI 27002: 2018 - Standard al Organizaţiei Internaţionale de Standardizare (ISO) pentru Securitatea Informatiei;
- Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei;
- Regulamentul (UE) 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date (Regulamentul general privind protecţia datelor - GDPR);
- Directiva (UE) 2016/680 referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii.

### *4.2. Legislaţie primară*

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

### 5.1. Definiţii ale termenilor specifici utilizati în activitatea reglementată de prezenta PO

| Nr. crt. | Termenul* | Definiţia şi/sau, dacă este cazul, actul normativ care defineşte termenul |
|---|---|---|
| 1. | ***Cont*** | O entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/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 informaţiei*** | Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei reţele indicând o posibilă încălcare a politicii de securitate a informaţiei, un eşec al mijloacelor de control sau o situaţie ignorată anterior dar care poate fi relevantă din punct de vedere al securităţii. |
| 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 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. |
| 6 | ***Incident privind securitatea informaţiei*** | Unul sau o serie de evenimente privind securitatea informaţiei nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operaţiunilor de business şi de ameninţare a securităţii informaţiei. |
| 7 | ***Internet*** | Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice. |
| 8 | ***Intranet*** | 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). |
| 9 | ***Protecţie informaţională*** | Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii. |
| 10 | ***Securitatea*** | Domeniul securităţii care prezintă atât măsuri pentru prevenire cât şi pentru împiedicarea atacatorilor să aibă acces la obiective, |

| | | |
|---|---|---|
| | ***fizică*** | 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 din Cluj 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** | Compartiment Salarizare |
| 8 | **CTA** | Compartiment Tehnic Administrativ |
| 9 | **CIT** | Compartiment IT |
| 10 | **CGT** | Compartiment Granturi |
| 11 | **BVC** | Buget de venituri si cheltuieli |
| 12 | **CAP** | Compartiment Achiziţii Publice |
| 13 | **CAPI** | Compartimentul de Audit Public Intern |
| 14 | **CJ** | Compartiment Juridic |
| 15 | **CSECR** | Compartiment Secretariat |
| 16 | **CREG** | Compartiment Registratură |
| 17 | **CMSCIM** | Comisia de monitorizare a Sistemului de Control Intern Managerial |
| 18 | **CtŞ** | Contabil şef al ARFCN |
| 19 | **CPA** | Compartiment Patrimoniu |
| 20 | **CRP** | Compartiment Relaţii Publice |
| 21 | **DAdj.ARFCN** | Director adjunct în cadrul ARFCN |
| 22 | **DI-ARFCN** | Directorul de institut/centru/colectiv de cercetare din cadrul ARFCN |
| 23 | **DP** | Directorul de proiect |
| 24 | **E** | Elaborare |
| 25 | **F** | Formular |
| 26 | **IL** | Instrucţiune de lucru |
| 27 | **PARFCN** | Preşedintele Filialei Cluj-Napoca a Academiei Române |
| 28 | **PCM** | Preşedintele Comisiei de Monitorizare |
| 29 | **PS** | Procedură de sistem |
| 30 | **PO** | Procedură operaţională |
| 31 | **SCIM** | Sistem de Control Intern Managerial |
| 32 | **V** | Verificare |
| 33 | **ILIL** | Institutul de Lingvistică şi Istorie Literară "Sextil Puşcariu" |
| 34 | **BARCJ** | Biblioteca Academiei Române – Filiala Cluj-Napoca |
| 35 | **IGB** | Institutul de Istorie "George Barițiu – Departamentul de Istorie |
| 36 | **DCSU** | Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane. |
| 37 | **CST** | Centrul de Studii Transilvane |
| 38 | **IAFAR** | Arhiva de Folclor a Academiei Române |
| 39 | **IAIA** | Institutul de Arheologie şi Istoria Artei |
| 40 | **CGC** | Colectivul de Geografie Cluj |
| 41 | **ICTP** | Institutul de Calcul „Tiberiu Popoviciu" |
| 42 | **OACJ** | Observatorul Astronomic Cluj |
| 43 | **ISER** | Institutul de Speologie "Emil Racoviță" – ColectivulCluj |

| | | |
|---|---|---|
| 44 | **ICSUMS** | Institutul de Cercetări Socio-Umane din Tg. Mureş |

## 6. DESCRIEREA PROCEDURII

În anumite situaţii este permisă utilizarea ocazională a sistemului informatic.

**În aceste situaţii se aplică următoarele restricţii:**

1. Utilizarea personală ocazională a serviciilor de poştă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.
2. Utilizarea ocazională a sistemului informatic nu trebuie să aibă drept rezultate costuri directe pentru ARFCN.
3. Utilizarea ocazională a sistemului informatic nu trebuie să afecteze activitatea normală a angajaţilor.
4. Furnizorii de bunuri şi servicii pot utiliza Sistemul Informatic al Academiei Române Filiala Cluj numai sub supravegherea unei persoane autorizate din cadrul Academiei Române Filiala Cluj-Napoca.
5. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva ARFCN sau prejudicierea, indiferent de formă, a intereselor ARFCN

### 6.1 Documente utilizate

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

### 6.2 Resurse necesare

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

### 6.3 Modul de lucru

**Planificarea operaţiunilor şi acţiunilor activităţii:**

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

## 7. RESPONSABILITĂŢII

**Coordonatorul IT are următoarele responsabilităţi şi competenţe:**

a) creează condiţiile de aplicare a prezentei procedurii;

b) monitorizează nivelul de securitate informaţională şi propune masuri de optimizare;

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 ARFCN 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 | | | | | |