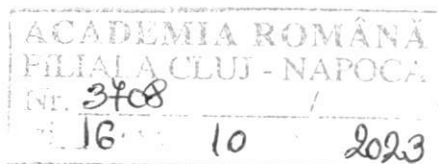


 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
	COD: PO-CIT-09	Pagina 1 din 14
		Exemplar nr. 1



APROB
PREȘEDINTE Filiala Cluj-Napoca



PROCEDURA OPERAȚIONALĂ
privind sistemul de Mesagerie Electronică
COD: PO-CIT-09

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 GOVACIU
Inspector de specialitate

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 2 din 14
	COD: PO-CIT-09	Exemplar nr. 1

1. CUPRINS

Numărul componentei în cadrul procedurii	Denumirea componentei din cadrul procedurii operaționale	Pagina
	Pagina de gardă	
1.	Cuprins	
2.	Scopul procedurii	
3.	Domeniu de aplicare	
4.	Documente de referință	
5.	Definiții și abrevieri	
6.	Descrierea activității sau procesului	
7.	Responsabilități	
8.	Formular de evidență a modificărilor	
9.	Formular de analiză a procedurii	
10.	Formular de distribuire/difuzare	
11.	Diagramă de proces	
12.	Documente utilizate	
13.	Anexe	

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
	COD: PO-CIT-09	Pagina 3 din 14
		Exemplar nr. 1

2. SCOPUL PROCEDURII

Acestea au ca scop principal modul de utilizare și transmitere în sistemul de mesagerie electronică în rețeaua internet și intranet ARFCN. De asemenea acestea au ca scop conectarea corectă a utilizatorilor autorizați în rețeaua proprie pentru ca informațiile prelucrate să fie folosite în scopuri academice și de cercetare, în scopul desfășurării activității specificate în fișa postului; Academiei Române și a investițiilor acesteia pentru dezvoltarea sistemului informatic.

Scopul acestei proceduri este acela de a asigura:

- Stocarea e-mail-urilor, documentelor și altor fișiere personale nu este încurajată;
- În cazul în care acestea sunt totuși păstrate, vor fi stocate local și nu pe serverele ARFCN, în locații separate de cele care conțin informații ce aparțin Filialei;
- Protejarea informațiilor Academiei Române Filiala Cluj-Napoca pentru dezvoltarea sistemului informatic;
- Protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate folosind sistemul Informatic a utilizatorilor autorizați: personal administrativ, cercetători, colaboratori etc.
- Educarea utilizatorilor privind modul de transmitere a mesajelor în rețeaua intranet și internet;
- Compatibilitate cu regulamentele, statutul și atribuțiile stabilite pentru administrarea sistemului informatic.
- Toate mesajele și fișierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Planul și Politica de Securitate a sistemului informatic din cadrul ARFCN.

2.1. Stabilește modul de transmitere a mesajelor în rețeaua ARFCN transmise prin intermediul resurselor informatice.

2.2. Dă asigurări cu privire la existența documentației adecvate derulării activității de rezolvare a unui incident de securitate.

2.3. Asigură continuitatea activității, inclusiv în condiții de fluctuație a personalului.

2.4. Sprijină auditul și/sau alte organisme abilitate în acțiuni de auditare și/sau control și pe conducătorii ARFCN în luarea deciziei.

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 4 din 14
	COD: PO-CIT-09	Exemplar nr. 1

3. DOMENIUL DE APLICARE

3.1 Precizarea (definirea) activității la care se referă procedura operațională:

Procedura se referă la modul de transmitere a mesageriei electronice în utilizarea rețelei intranet și internet în sistemul informatic realizată de personalul ARFCN stabilind totodată regulile, normele și măsuri le de prevenire și combatere a incidentelor de securitate.

3.2 Scopul administrării sistemului informatic, privind asigurarea securității acestuia, în conformitate cu legile în vigoare.

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 derulării 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 Informației; Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;

- ISO/CEI 27002: 2018 - Standard al Organizației Internaționale de Standardizare (ISO) pentru Securitatea Informației;

- 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

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 5 din 14
	COD: PO-CIT-09	Exemplar nr. 1

private în cadrul comunicațiilor electronice;

- Ordonanța de Guvern nr.124/2000 (TI) - pentru completarea cadrului juridic privind dreptul de autor și drepturile conexe, prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio și video, precum și a programelor pentru calculator;

- Legea 213/2002 (TI) - privind aprobarea Ordonanței Guvernului nr. 124/2000 pentru completarea cadrului juridic privind dreptul de autor și drepturile conexe prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio și video, precum și a programelor pentru calculator;

- Legea nr. 135/2007, legea privind arhivarea documentelor în forma electronică;

- HG 58/1998 – pentru aprobarea Strategiei naționale de informatizare și implementare în ritm accelerat a societății informaționale și a Programului de acțiuni privind utilizarea pe scară largă și dezvoltarea sectorului tehnologiilor informației 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 și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

- Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

- OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităților publice

- Ghidul de securitate informatică pentru funcționarii publici, CERT-RO;

4.3. Legislație secundară

- a. Statutul Academiei Române;

- b. Legea nr. 752/2001 privind organizarea și funcționarea Academiei Române cu modificările și completările ulterioare

4.4. Alte documente, inclusiv reglementări interne ale entității publice

- a. Regulamentul Intern al Academiei Române Filiala Cluj-Napoca;

- b. Regulamentul de Organizare și Funcționare al Academiei Române Filiala Cluj-Napoca;

- c. PS – ARFC 00

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia —
		Pagina 6 din 14
	COD: PO-CIT-09	Exemplar nr. 1

5. DEFINIȚII ȘI ABREVIERI

a. Definiții ale termenilor specifici utilizați 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 informații privind o persoană fizică identificată sau identificabilă (persoana vizată); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității 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		Acțiuni întreprinse în vederea afectării informațiilor și sistemelor

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 7 din 14
	COD: PO-CIT-09	Exemplar nr. 1

	Protecție informațională	informatică 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 ARFC cuprinde resursele informatice și de comunicații ale ARFC.
15	Stocarea Externă (Offsite)	Stocarea externă trebuie să se realizeze într-o zonă geografică diferită de sediul ARFC 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/locăție securizată din ARFC 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 (<i>Personal Digital Assistant</i> - PDA), smartphone-uri, pagere, sisteme de

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

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 8 din 14
	COD: PO-CIT-09	Exemplar nr. 1

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
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	CompartimentJuridic
16	CSECR	Compartiment Secretariat
17	CREG	Compartiment Registratură
18	CMSCIM	Comisia de monitorizare a Sistemului de Control Intern Managerial
19	CtŞ	Contabil şef al ARFC
20	DAdj.ARFC	Director adjunct în cadrul ARFC
21	DI-ARFC	Directorul de institut/centru/colectiv de cercetare din cadrul ARFC
22	DP	Directorul de proiect
23	E	Elaborare
24	F	Formular
25	IL	Instrucțiune de lucru
26	PARFC	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



Academia Română - Filiala Cluj-Napoca
COMPARTIMENT IT

Procedura operațională

**privind sistemul de Mesagerie
Electronică**

COD: PO-CIT-09

Ediția I

Revizia __

**Pagina
9 din 14**

Exemplar nr. 1

DESCRIEREA PROCEDURII

- ✓ Adresa de e-mail instituțională furnizată de ARFCN și mailbox-ul asociat acesteia, adresa IP și, după caz, numărul de telefon fix, telefon mobil și conexiunea de date mobile sunt resurse puse la dispoziția utilizatorilor ARFCN pentru a fi folosite la îndeplinirea sarcinilor de serviciu.
- ✓ Utilizarea ocazională în scop personal a acestora este permisă numai dacă nu afectează într-o măsură perceptibilă consumul de resurse al ARFCN și nu introduce riscuri suplimentare pentru Filială.
- ✓ ARFCN nu își asumă nicio responsabilitate cu privire la securitatea acestor informații, întreaga responsabilitate (inclusiv realizarea copiilor de siguranță) revenind utilizatorului.

1. Următoarele activități sunt strict interzise utilizatorilor:

- Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
- Folosirea sistemului de mesagerie electronică în scopuri personale;
- Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate. Procurarea și distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci și logo-uri ale altor companii preluate din reviste, ziare, cărți sau de pe internet);
- Folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de support administrativ. Falsificarea, denaturarea, ascunderea, suprimarea sau înlocuirea unei identități de utilizator, pe orice mijloc de comunicare electronică, cu scopul de a induce în eroare destinatarul cu privire la identitatea expeditorului;
- Utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităților ilegale, procurarea și distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărțuire, defăimare sau amenințare;
- Trimiterea de spam sau bombe e-mail prin intermediul sistemului de e-mail, mesajelor text, mesageriei instant, mesageriei vocale sau altor forme de comunicare electronică utilizate;
- Transmiterea de informații confidențiale sau secrete de serviciu altor destinatari decât cei autorizați să primească aceste informații;
- Utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relații de afaceri care nu implică sau sunt contrare intereselor Academiei Române Filiala Cluj-Napoca din campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea Academiei Române Filiala Cluj-Napoca;
- Postarea sau transmiterea de mesaje non-business identice sau similare către un număr mare de destinatari (news-group spam);
- Utilizarea adresei de e-mail sau a adresei ip pentru a se angaja în activități care încalcă politicile sau orientările filialei; postarea pe grupuri publice de știri, forumuri sau rețele sociale folosind adresa de e-mail sau adresa ip ale ARFCN, reprezintă instituția în fața publicului și prin urmare trebuie efectuată cu discernământ pentru a evita reprezentarea greșită sau depășirea autorității de a reprezenta poziția ARFCN;

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
		Pagina 10 din 14
	COD: PO-CIT-09	Exemplar nr. 1

6.1 Compartimentul IT are la bază următoarele obiective:

- ✓ să nu permită trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deserveșc instituția;
- ✓ să nu permită trimiterea mesajelor de dimensiuni foarte mari;
- ✓ să nu permită trimiterea sau retrimiteră mesajelor ce pot conține viruși;
- ✓ să nu trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc ARFCN, folosind dispozitive de comunicații mobile care nu sunt autorizate de ARFCN. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenți digitali personali, pagere ce permit trimiterea/primirea de informații și telefoanele mobile.
- ✓ să nu permită angajaților încălcarea drepturilor de autor sau a contractelor de licențe vor duce la sancțiuni disciplinare din partea ARFCN și/sau acțiuni în instanță ale deținătorului dreptului de autor.

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 și acțiunilor activității:

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

6.5 Derularea operațiunilor și acțiunilor activității:

- orice mesaj și/sau informație trimisă prin intermediul rețelilor publice pot fi identificate și atribuite Academiei Române Filiala Cluj-Napoca-Napoca. Din acest motiv, postarea pe forumuri sau alte site-uri de informații care implică numele sau adrese de e-mail ale ARFCN se va face fără furnizarea de informații confidențiale sau care pot afecta reputația ARFCN. Părerile personale exprimate pe astfel de site-uri sau forumuri vor fi însoțite de nota: "Părerile exprimate sunt personale și nu reprezintă poziția oficială a Academiei Române Filiala Cluj-Napoca".

RESPONSABILITĂȚI

Coordonatorul IT are următoarele responsabilități și competențe:

- a) creează condițiile de aplicare a prezentei procedurii;
- b) monitorizează modul de folosire și de implementare privind sistemul de mesagerie electronica și propune masuri de optimizare a acestora;
- c) numește responsabili care să asigure elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind sistemul de Mesagerie Electronică	Revizia __
	COD: PO-CIT-09	Pagina 11 din 14
		Exemplar nr. 1

d) urmărește modul de utilizare, conectare în rețeaua intranet și internet la nivel de Institute/ Centre /Colective.

Oficiul Juridic are următoarele responsabilități și competențe:

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

Președintele ARFC 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.

3. 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					