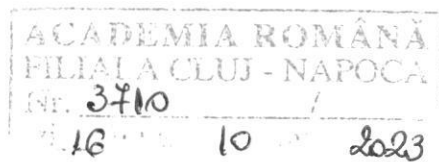


 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind rezolvarea incidentelor de securitate	Revizia ____
		Pagina 1 din 13
	COD: PO-CIT-06	Exemplar nr. 1



APROB
PREȘEDINTE Filiala Cluj-Napoca


Doru PAMEL

PROCEDURA OPERAȚIONALĂ
privind rezolvarea incidentelor de securitate
COD: PO-CIT-06

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



 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind rezolvarea incidentelor de securitate	Revizia ____
		Pagina 2 din 13
	COD: PO-CIT-06	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 rezolvarea incidentelor de securitate	Revizia __
		Pagina 3 din 13
	COD: PO-CIT-06	Exemplar nr. 1

2. SCOPUL PROCEDURII

Acestea au ca scop principal rezolvarea unor incidente de securitate care se produc în rețeaua ARFCN de orice tip (cu sau fără intenție). De asemenea acestea au ca scop protejarea imaginii Academiei Române și a investițiilor acesteia pentru dezvoltarea sistemului informatic. Scopul acestei proceduri este acela de a asigura:

- Confidențialitatea informațiilor transmise prin intermediul resurselor informatice ale terților nu poate fi asigurată/garantată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare;
- Șefii entităților organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la RIC ale ARFCN. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele și datele de identificare ale acesteia se vor comunica către Responsabilul IT;
- Protejarea imaginii Academiei Române Filiala Cluj-Napoca;
- 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 sistemului informatic în ceea ce privește incidentele de securitate;
- Compatibilitate cu regulamentele, statutul și atribuțiile stabilite pentru administrarea sistemului informatic.

2.1. Stabilește modul de rezolvare a unor incidente de securitate care se produc 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 rezolvarea incidentelor de securitate	Revizia ____
		Pagina 4 din 13
	COD: PO-CIT-06	Exemplar nr. 1

3. DOMENIUL DE APLICARE

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

Procedura se referă la modul de rezolvare a unui incident de securitate în sistemul informatic realizată de personalul ARFCN stabilind totodată regulele, 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 rezolvarea incidentelor de securitate	Revizia __
		Pagina 5 din 13
	COD: PO-CIT-06	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 rezolvarea incidentelor de securitate	Revizia __
	COD: PO-CIT-06	Pagina 6 din 13
		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 rezolvarea incidentelor de securitate	Revizia __
	COD: PO-CIT-06	Pagina 7 din 13
		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/locație 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 rezolvarea incidentelor de securitate	Revizia __
		Pagina 8 din 13
	COD: PO-CIT-06	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	Compartiment Salarizare
8	CTA	Compartiment Tehnic Administrativ
9	CIT	Compartiment IT
	CGT	Compartiment Granturi
10	BVC	Buget de venituri si cheltuieli
11	CAP	Compartiment Achiziții Publice
12	CAPI	Compartimentul de Audit Public Intern
13	CJ	Compartiment Juridic
14	CSECR	Compartiment Secretariat
15	CREG	Compartiment Registratură
16	CMSCIM	Comisia de monitorizare a Sistemului de Control Intern Managerial
17	Ctș	Contabil șef al ARFC
18	DAdj.ARFC	Director adjunct în cadrul ARFC
19	DI-ARFC	Directorul de institut/centru/colectiv de cercetare din cadrul ARFC
20	DP	Directorul de proiect
21	E	Elaborare
22	F	Formular
23	IL	Instrucțiune de lucru
24	PARFC	Președintele Filialei Cluj-Napoca a Academiei Române
25	PCM	Președintele Comisiei de Monitorizare
26	PS	Procedură de sistem
27	PO	Procedură operațională
28	SCIM	Sistem de Control Intern Managerial
29	V	Verificare
30	ILIL	Institutul de Lingvistică și Istorie Literară "Sextil Pușcariu"
31	BARCJ	Biblioteca Academiei Române – Filiala Cluj-Napoca
32	IGB	Institutul de Istorie "George Barițiu – Departamentul de Istorie
33	DCSU	Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane
34	CST	Centrul de Studii Transilvane
35	IAFAR	Arhiva de Folclor a Academiei Române
36	IAIA	Institutul de Arheologie și Istoria Artei
37	CGC	Colectivul de Geografie Cluj
38	ICTP	Institutul de Calcul „Tiberiu Popoviciu”
39	OACJ	Observatorul Astronomic Cluj
40	ISER	Institutul de Speologie "Emil Racoviță" – Colectivul Cluj
41	ICSUMS	Institutul de Cercetări Socio-Umane din Tg. Mureș

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind rezolvarea incidentelor de securitate	Revizia __
		Pagina 9 din 13
	COD: PO-CIT-06	Exemplar nr. 1

DESCRIEREA PROCEDURII

- ✓ Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activități suspecte, informații modificate etc., trebuie urmate procedurile standard specifice pentru micșorarea riscurilor;
- ✓ RSSI este responsabil cu coordonarea pentru tratarea incidentului;
- ✓ RSSI este responsabil cu strângerea dovezilor fizice și electronice ce vor face parte din documentația pentru tratarea incidentului;
- ✓ RSSI este responsabil de coordonarea activităților de comunicare cu Compartimentul IT;
- ✓ Achiziții pentru rezolvarea incidentului;
- ✓ În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare RSSI va recomanda sancțiuni disciplinare;
- ✓ În cazul în care incidentul implică aplicarea legilor civile sau penale DPO/RSSI va recomanda sesizarea organelor în drept ale statului și va acționa ca ofițer de legătură cu aceste.

6.1 Compartimentul IT are la bază următoarele obiective:

- ✓ să intervină și să rezolve orice problemă apărută în sistemul informatic al ARFCN și să fie în măsură să aplice procedurile legale în urma producerii unui incident de securitate;
- ✓ să stîngă dovezi fizice și electronice privitor la producerea incidentului de securitate și să le comunice șefului entității;
- ✓ să ia măsuri de combatere a producerii unui incident de securitate aplicînd politici de securitate în SI la nivel ARFCN;

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:

1. 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.

2. Utilizatorii vor avea grijă să nu încalce drepturile de confidențialitate ale altor persoane

 Academia Română - Filiala Cluj-Napoca COMPARTIMENT IT	Procedura operațională	Ediția I
	privind rezolvarea incidentelor de securitate	Revizia __
		Pagina 10 din 13
	COD: PO-CIT-06	Exemplar nr. 1

atunci când utilizează echipamentele (de exemplu, când fac înregistrări audio-video la locul de muncă);

3. Utilizatorul trebuie să se asigure prin mijloace legale că nu încalcă regulile și că informațiile aparținând sau aflate în custodia Academiei Române Filiala Cluj-Napoca rămân sub controlul ARFCN în orice moment;

4. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității sistemului informatic.

RESPONSABILITĂȚII

Coordonatorul IT are următoarele responsabilități și competențe:

- a) creează condițiile de aplicare a prezentei proceduri;
- b) monitorizează nivelul de conectare a userilor precum și modul de implementare privind securitate informațională și propune măsuri de optimizare a acestora;
- c) numește responsabili care să asigure elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;
- d) urmărește să nu se producă incidente de securitate aplicând politicii de securitate la nivel informațional atunci când utilizează echipamentele ARFCN.

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					