ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
Nr. 3404 /
16 10 2023

APROB
PREŞEDINTE Filiala Cluj-Napoca

Doru PAMFIL

PROCEDURA OPERAŢIONALĂ
privind modul de detecţie a Viruşilor
COD: PO–CIT-10

Ediţia I, Revizia 0, Data 26.09.2023

Avizat
Preşedinte Comisiei de Sistem de Control Managerial Intern

Lucian CUIBUS

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

Elaborat,
Adrian COVACIU
Inspector de specialitate

1. CUPRINS

2. SCOPUL PROCEDURII

Acestea au ca scop principal modul de prevenire, combatere și detecție a virușiilor în rețeaua 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 intacte din punct de vedere informațional și folosite în scopuri academice și de cercetare, în scopul desfășurării activității specificate în fișa postului;

Scopul acestei proceduri este acela de a asigura:

- Stocarea tuturor informațiilor, e-mail-urilor, documentelor și altor fișiere personale în deplină siguranță fără să fie alterate;
- Protejarea informațiilor Academiei Române Filila 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 utilizare a pachetelor antivirus dispuse la dispoziția utilizatorului în rețeaua intranet și internet;.
- Toate mesajele și fișierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Planul si Politica de Securitate a sistemului informatic din cadrul ARFCN.

2.1. Stabilește modul de de prevenire, combatere și detecție a virușiilor 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.

3. DOMENIUL DE APLICARE

3.1 **Precizarea (definirea) activității la care se referă procedura operațională:** Procedura se referă la modul de de prevenire, combatere și detecție a virușiilor în utilizarea rețelei intranet și internet în sistemul informatic realizată de personalul ARFCN stabilind totodată reguile, 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 Informatiei; Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;
- ISO/CEI 27002: 2018 - Standard al Organizației Internaționale de Standardizare (ISO) pentru Securitatea Informatiei;
- Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;
- Regulamentul (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor - GDPR)
- Directiva (UE) 2016/680 referitoare la protecția datelor personale în cadrul activităților

specifice desfășurate de autoritățile de aplicare a legii

4.2. Legislație primară

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

private în cadrul 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

5. DEFINIŢII ŞI ABREVIERI

a. 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		Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor

	Protecție informațională	informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii.
10	***Securitatea fizică***	Domeniul securității care prezintă atât măsuri pentru prevenire cât și pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informații și recomandări privind proiectarea infrastructurii pentru a opune rezistență la actele ostile.
11	***Securitatea informației***	Set de măsuri tehnice și organizatorice care au ca scop asigurarea păstrarea confidențialității, integrității și a disponibilității informației.
12	***Semnătură electronică***	Atribut indispensabil al documentului electronic, obținut în urma transformării criptografice a acestuia, cu utilizarea cheii private, conform prevederilor Legii nr. 455/2001 privind semnătura electronică, republicată.
13	***Server***	Un program de calculator care oferă servicii altor programe aflate pe același calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe același calculator mai pot rula și alte programe de tip client sau server.
14	***Sistem informatic***	Set integral de componente pentru colectarea, stocarea, prelucrarea datelor și informațiilor pentru furnizarea lor, cunoștințelor și a produselor digitale. Componentele unui sistem informatic sunt hardware, software, telecomunicații, datele prelucrate, baze de date, resurse umane, precum și proceduri. Sistemul informatic al 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 (*Personal Digital Assistant* - PDA), smartphone-uri, pagere, sisteme de

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

b. Abrevieri

Nr. crt.	Abreviere	Termenul abreviat
1	**A**	Aprobare
2	**Ah.**	Arhivare
3	**Ap.**	Aplicare
4	**ARFC**	Academia Română - Filiala Cluj-Napoca
5	**CFC**	Compartiment Financiar -Contabilitate
6	**CRU**	Compartiment Resurse Umane
7	**CSAL**	CompartimentSalarizare
8	**CTA**	Compartiment Tehnic Administrativ
9	**CIT**	Compartiment IT
10	**CGT**	Compartiment Granturi
11	**CSSM**	Compartiment Securitate şi Sănătate în Muncă
12	**BVC**	Buget de venituri si cheltuieli
13	**CAP**	Compartiment Achiziţii 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**	Instrucţiune 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 operaţională
30	**SCIM**	Sistem de Control Intern Managerial
31	**V**	Verificare
32	**ILIL**	Institutul de Lingvistică şi Istorie Literară "Sextil Puşcariu"
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

DESCRIEREA PROCEDURII

✓ Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Academiei Române Filiala Cluj-Napoca, trebuie să utilizeze programe antivirus aprobate de către RSSI;
✓ Programele antivirus nu trebuie dezactivate;
✓ Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului;
✓ Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator;
✓ Orice server de fişiere conectat la reţeaua Instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie;
✓ Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program;
✓ Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat la RSSI.

6.1 Compartimentul IT are la bază următoarele obiective:

✓ să instaleze pe toate staţiile / dispozitive, medii amovibile protecţie antivirus;
✓ să actualizeze zilnic pe toate staţiile independente noiile semnături de protecţie antivirus;
✓ să nu permită trimiterea sau retrimiterea mesajelor ce pot conţine viruşi;
✓ să nu trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc ARFCN, folosind dispozitive de comunicaţii mobile care nu sunt scanate şi autorizate de ARFCN. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile.
✓ să nu permită angajaţilor încălcarea drepturilor de autor sau a contractelor de licenţe vor duce la sancţiuni disciplinare din partea ARFCN şi/sau acţiuni în instanţă ale deţinătorului 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:

Operațiunile 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 rețelelor 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".

RESPONSABILITĂȚII

Coordonatorul IT are următoarele responsabilități și competențe:

a) creează condițiile de aplicare a prezentei procedurii;

b) monitorizează modul de folosire și de implementare privind modul de scanare a tuturor informațiilor aflate în rețeaua ARFCN;

c) numește responsabili care să asigure punerea în aplicare în elaborarea / modificarea și gestionarea procedurilor specifice în cadrul serviciului;

Oficiul Juridic are următoarele responsabilități și competențe:

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

Președintele ARFCN are următoarele responsabilități și competențe:

a) avizează PS și PO elaborate;

b) conciliază aspecte neclare în relația realizator – avizator și ia decizia finală în cazul lipsei consensului dintre realizator – avizatori.

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					