ACADEMIA ROMÂNĂ
FILIALA CLUJ - NAPOCA
Nr. 2442 /
zi 22 luna 07 an 2021

APROB
PREȘEDINTE Filiala Cluj-Napoca

Doru PAMFIL

Plan de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca

COD: PS–ARFCN.00

Ediția I, Revizla 0, Data 20.07.2021

Avizat,

Președinte Comisiei de Sistem de Control Managerial Intern

Claudiu CRISTUREAN

Verificat,

[Nume și prenume conducător compartiment/institut]

[Data și semnătura]

Elaborat,

Adrian COVACIU responsabilă de activitate]

17.07.2021

1. CUPRINS

2. INTRODUCERE

Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Informatic al Academiei Română Filiala Cluj-Napoca.

Regulile şi procedurile din planul de securitate (vezi anexele prezentului Plan) au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în aşa fel încât fiecare să poată fi folosită cvasiindependent de celelalte.

În acord cu lcgislaţia în vigoare în România, Regulamentul de ordine interioară al Academiei Române Filiala Cluj-Napoca, resursele Sistemului Informatic sunt valori ale Academiei Române Filiala Cluj-Napoca care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român.

3. SCOP

Regulamentele de utilizare a Sistemului Informatic sunt elaborate pentru a stabili un cadru procedural corect, legal şi eficient de utilizare a tehnologiei informaţiei în Academia Română Filiala Cluj-Napoca.

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 Filiala Cluj-Napoca şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic.

Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea sistemului informatic al ARFCN în vederea îndeplinirii misiunii şi a obiectivelor instituţionale şi individuale;

- Protejarea imaginii Academiei Române Filila Cluj-Napoca;
- Protejarea investiţiilor Academiei Române Filila Cluj-Napoca pentru dezvoltarea sistemului informatic;
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Sistemul Informatic a utilizatorilor autorizaţi: personal administrativ, cercetători, colaboratori etc.
- Educarea utilizatorilor sistemului informatic în ceea ce priveşte responsabilităţile asociate cu utilizarea acestuia;
- Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea sistemului informatic.

4. AUDIENȚĂ

Planul de Securitate privind utilizarea Sistemului Informatic al Academiei Române Filiala Cluj-Napoca se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la SI- ARFCN.

Categoriile de persoane care au acces la SI-ARFCN sunt:

- angajații ARFCN care pentru îndeplinirea sarcinilor de serviciu folosesc în activitatea lor sistemul informatic;
- colaboratorii ARFCN;
- angajații firmelor de prestări servicii cu care ARFCN colaborează (furnizorii de servicii IT);

5. DOCUMENTE DE REFERINȚĂ

5.1. Reglementări internaţionale

5.1.1. ISO 17799 – Standard al Organizaţiei Internaţionale de Standardizare (ISO) ce conţine recomandări privitoare la securitatea digitală. http://www.iso17799software.com/what.htm;

5.1.2. 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,

5.1.3. 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;

5.1.4. 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)

5.1.5. Directiva (UE) 2016/680 referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii

5.2. Legislaţia primară

5.2.1. Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe;

5.2.2. Legea nr. 455 din 18 iulie 2001 privind semnătura electronică;

5.2.3. Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public;
5.2.4. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
5.2.5. Legea nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate;
5.2.6. Hotărârea nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
5.2.7. Legea 506/2004 (TI) - privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în cadrul comunicaţiilor electronice;
5.2.8. 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;
5.2.9. 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;
5.2.10. Legea nr. 135/2007, legea privind arhivarea documentelor în forma electronică;
5.2.11. 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;
5.2.12. 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)
5.2.13. 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)
5.2.14. Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice
5.2.15. OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice
5.2.16. Ghidul de securitate informatică pentru funcţionarii publici, CERT-RO;

5.3. <u>Alte documente, inclusiv reglementări interne ale entităţii publice</u>

5.3.1. Regulamentul Intern al Academiei Române Filiala Cluj-Napoca;
5.3.2. Regulamentul de Organizare şi Funcţionare al Academiei Române Filiala Cluj-Napoca;
5.3.3. Politica de Securitate privind Sistemul Informatic din cadrul Academiei Române Filiala Cluj-Napoca;
5.3.4. Ghidul de utilizare a conturilor de e-mail instituţionale în cadrul ARFCN;
5.3.5. Politica internă de protecţie a datelor cu caracter personal.

6. DEFINIȚII ȘI ABREVIERI ALE TERMENILOR UTILIZAȚI ÎN PLANUL DE SECURITATE

6.1. Definiții ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	***Abuz de privilegii***	Orice acțiune întreprinsă în mod voit de un utilizator, care vine in contradicție cu regulamentele Academiei Române Filiala Cluj-Napoca și/sau legile in vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.
2.	**Amenințare**	Cauză potențială a unui incident nedorit care poate produce daune unui sistem sau organizații.
3.	***Atac informațional***	O încercare de a trece peste măsurile și controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului informatic pentru a distruge, a expune, a modifica, a dezactiva, a fura sau a obține accesul neautorizat sau a utiliza în mod neautorizat o resursă. Atacatorul poate altera informațiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular și de eficacitatea contramăsurilor aplicate.
4.	***Cal troian***	Virus sau vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fișier de pe o pagină Web sau un forum.
5.	***Copii de Siguranță (backup)***	Copii ale fișierelor și aplicațiilor făcute pentru a evita pierderea datelor și pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.
6.	***Cont***	O entitate specificată printr-un identificator și/sau parolă pentru accesul la sistemul de comunicație și/sa la o resursă de calcul.
7.	***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.
8.	***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.
9.	***Firewall***	Un mecanism de control al accesului care acționează ca o barieră

		între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.
10.	***Furnizor***	Persoană fizică/juridică care oferă bunuri sau servicii Academiei Romană Filiala Cluj-Napoca în baza unui contract comercial sau de colaborare.
11.	***Gazdă (Host)***	Un sistem care oferă servicii pentru un anumit număr de utilizatori.
12.	***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.
13.	***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.
14.	***Internet***	Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.
15.	***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).
16.	***Medii de stocare***	Echipamente, dispozitive (hardware) de stocare a informaţiilor în format electronic. Exemple: Hard-disk-ul (HDD), unităţi optice (CD, DVD, Blu-Ray), carduri de memorie: Compact Flash (CF), EEPROM (Electrically Erasable Programmable Read-Only Memory), Memorie Flash, Memory Stick (MS), Memory Stick Duo, Memory Stick Micro, Memory Stick PRO-HG, Memory Stick XC, Microdrive, Nand Flash NOR Flash, Pen Drive / Flash Drive / Key Drive / Memorie USB, Secure Digital (SD), Mini Secure Digital (Mini SD) SIM Card, SmartMedia (SM), Transflash, XD. Detalii suplimentare pentru carduri de memorie se găsesc la adresa: carduridememorie
17.	***Protecţie informaţională***	Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.
18.	***Responsabil cu Securitatea***	Este angajatul ARFCN care are reponsabilităţi privind securitatea.

19.	***Sistemului Informatic (RSSI):***	Responsabilii IT din cadrul tuturor structurilor din organigrama ARFCN numiți prin decizie a PARFCN.
20.	***Rețea locală (LAN)***	O rețea de comunicații de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Rețeaua locală oferă comunicații între calculatoare și periferice la o viteză de transfer mare și cu puține erori.
21.	***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.
22.	***Securitatea informației***	Set de măsuri tehnice și organizatorice care au ca scop asigurarea păstrarea confidențialității, integrității și a disponibilității informației.
23.	***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.
24.	***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.
25.	***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.
26.	***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.
27.	***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

		procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.
27.	***Utilizator***	Angajat al ARFCN care pentru îndeplinirea sarcinilor de serviciu foloseşte în activitatea sa sistemul informatic al ARFCN. O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către ARFCN, în conformitate cu procedurile şi regulamentele în vigoare, să folosească sistemul informatic.
28.	***Vierme***	Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.
29.	***Virus***	Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.
30.	**Vulnerabilitate**	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o ameninţare.

6.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1	**ARFCN**	Academia Română Filiala Cluj-Napoca
2	**PARFCN**	Preşedintele Filialei Cluj-Napoca a Academiei Române
3	**DAdj.ARFCN**	Director adjunct în cadrul ARFCN
4	**CAPI**	Compartimentul de Audit Public Intern

5	**CJ**	Consilier Juridic
6	**CSECR**	Compartiment Secretariat
7	**CRU**	Compartiment Resurse Umane
8	**CREG**	Compartiment Registratură
9	**CtŞ**	Contabil şef al ARFCN
10	**CFC**	Compartiment Financiar și Contabilitate
11	**CSAL**	Compartiment Salarizare
12	**CAP**	Compartiment Achiziţii Publice
13	**CTA**	Compartiment Tehnic Administrativ
14	**CSSM-SU**	Compartiment Securitate și Sănătate în Muncă / Situații de Urgență
15	**CIT**	Compartiment IT
16	**BVC**	Buget de venituri și cheltuieli
17	**SCIM**	Sistem de Control Intern Managerial
18	**CMSCIM**	Comisia de monitorizare a Sistemului de Control Intern Managerial
19	**PCM**	Preşedintele Comisiei de Monitorizare
20	**DI-ARFCN**	Directorul de institut/Director Biblioteca Academiei din Cluj-Napoca/Șef de colectiv din cadrul ARFCN
21	**DP**	Directorul de proiect
22	**PS**	Procedură de sistem
23	**PO**	Procedură operaţională
24	**Apr.**	Aprobare
25	**Ah.**	Arhivare
26	**Apl.**	Aplicare
27	**El.**	Elaborare
28	**Frm.**	Formular
29	**IL**	Instrucțiune de lucru
30	**Vf.**	Verificare
31	**OSGG**	Ordinul Secretariatului General al Guvernului
32	**BARC**	Biblioteca Academiei Române – Filiala Cluj-Napoca
33	**IIGB**	Institutul de Istorie "George Barițiu – Departamentul de Istorie

34	**DCSU**	Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane
35	**CST**	Centrul de Studii Transilvane
36	**IAIA**	Institutul de Arheologie și Istoria Artei
37	**ILIL**	Institutul de Lingvistică și Istorie Literară "Sextil Pușcariu"
38	**IAFAR**	Arhiva de Folclor a Academiei Române
39	**ICSUMS**	Institutul de Cercetări Socio-Umane și Biblioteca Târgu-Mureș
40	**OAC**	Observatorul Astronomic Cluj
41	**ISER**	Institutul de Speologie "Emil Racoviță" – Colectivul Cluj
42	**CCG**	Centrul de Cercetări Geografice Cluj
43	**ICTP**	Institutul de Calcul „Tiberiu Popoviciu"

52.	**OACJ**	Observatorul Astronomic Cluj
53.	**ISER**	Institutul de Speologie "Emil Racoviță" – ColectivulCluj
54.	**ICSUMS**	Institutul de Cercetări Socio-Umane din Tg. Mureș

7. PROCEDURI DE ELABORARE, MODIFICARE ȘI APROBARE A REGULAMENTULUI

1. Regulamentele şi/sau procedurile de utilizare a Sistemului informatic al Academiei Române Filiala Cluj-Napoca se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare regulament să poată fi folosit cvasi-independent de celelalte.
2. Regulamentele vor fi elaborate de către RSSI (Responsabil cu Securitatea Sistemului Informatic) al Academiei Române Filiala Cluj-Napoca şi vor fi propuse pentru aprobare conducerii ARFCN.
3. Modificarea prevederilor unui Regulament se face cu aprobarea conducerii ARFCN. Fiecare modificare va include modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioara rămâne valabilă până în momentul în care noua versiune este aplicabilă.
4. Prezentul document conţine o listă a tuturor regulamentelor aplicabile în Sistemul Informatic al ARFCN prezentată în cap.8.

8. LISTA PROCEDURILOR ȘI REGULAMENTELOR SPECIFICE SECURITĂȚII SI - ARFCN

1. Utilizarea permanentă a resurselor Informatice şi de Comunicaţii (Anexa nr. 1);
2. Utilizarea ocazională a resurselor Informatice şi de Comunicaţii (Anexa nr. 2);
3. Reguli privind accesul fizic la resursele Informatice şi de Comunicaţii (Anexa nr. 3);
4. Reguli de acces la reţeaua de comunicaţii (Anexa nr. 4);
5. Regulament privind confidenţialitatea serviciilor Informatice (Anexa nr. 5);
6. Regulament de tratare a incidentelor de Securitate (Anexa nr. 6);
7. Regulament privind crearea şi utilizarea copiilor de siguranţă (Backup) (Anexa nr.7);
8. Regulament de utilizare a reţelei Internet şi Intranet (Anexa nr. 8);
9. Regulament privind sistemul de Mesagerie Electronică (Anexa nr. 9);
10. Regulament de detectare a Viruşilor (Anexa nr. 10);
11. Regulament privind utilizarea dispozitivelor mobile (Anexa nr.11);
    11.1 Reguli privind securitatea informaţiilor în cazul utilizării echipamentelor portabile de tip laptop
    11.2 Reguli privind utilizarea echipamentelor portabile de tip tabletă şi smartphone
12. Regulament pentru parolele de acces (Anexa nr.12);
13. Regulament privind administrarea conturilor (Anexa nr.13);
14. Securitatea echipamentelor şi resurselor în afara locației ARFCN (Anexa nr.14);
15. Utilizarea echipamentelor proprietate personală (Anexa nr.15);
16. Regulament de acces la distanţă (Anexa nr.16);
17. Politica biroului curat şi a ecranului curat (Anexa nr. 17);
18. Securitatea fizică a echipamentelor IT (Anexa nr. 18);
19. Păstrarea, distrugerea şi eliminarea suporturilor informaționale (Anexa nr. 19);
20. Relaţii cu terţi (Anexa nr. 20);

21. Licențe de utilizare (Anexa nr. 21);

22. Returnarea resurselor la terminarea contractului (Anexa nr. 22);

23. Lista programelor de tip shareware sau freeware (Anexa nr. 23);

24. Lista aplicațiilor software permise a fi folosite în cadrul Academiei Române Filiala Cluj-Napoca (Anexa nr. 24).

9. RESPONSABILITĂȚII

9.1. Forurile decizionale ale Academiei Române Filiala Cluj-Napoca

Forurile decizionale ale ARFCN au următoarele responsabilități:

- aprobă Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca, procedurile și regulamentele asociate;
- asigură disponibilitatea resurselor necesare pentru aplicarea politicilor și procedurilor de securitate a sistemului informatic al ARFCN;
- comunică importanța unei gestionări eficiente a sistemelor informatice și de comunicații.

9.2. Conducerea Institutelor /centrelor/colectivelor:

- se asigură că sistemele informatice și de comunicații sunt gestionate eficient;
- îndrumă și sprijină personalul să contribuie la eficacitatea sistemelor informatice și de comunicații.

Șefii entităților organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a Planului de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca și a procedurilor și regulamentelor aferente acestuia;
- asigură că măsurile de securitate tehnice, fizice și procedurale adecvate sunt implementate în conformitate cu Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca;
- sunt aplicate în mod corespunzător de către tot personalul, asigurarea resurselor și efectuarea analizelor necesare pentru a se asigura că informațiile și activele sunt protejate în mod corespunzător în zona lor de responsabilitate,
- informarea persoanei desemnate cu managementul incidentelor de securitate despre încălcările reale sau presupuse ale Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca care afectează securitatea informațiilor din zona lor de responsabilitate (incidentele de securitate a informațiilor),
- identificarea și clasificarea informațiilor și echipamentelor din zona lor de responsabilitate și desemnarea deținătorilor (responsabililor) pentru acestea;
- informarea Compartimentului IT la schimbarea responsabililor de active informaționale (inclusiv schimbarea responsabililului IT din cadrul Institutelor/Centrelor/Colectivelor ARFCN.

9.3. Compartimentul IT (prin angajatul său)/responsabilii IT din cadrul Institutelor/Centrelor/Colectivelor ARFCN au următoarele reponsabilități:

- propun modificări ale Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române FilialaCluj;
- elaborează și propune pentru aprobare politici și proceduri de gestionare și de securitate a resurselor informatice și de comunicații în conformitate cu Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca;
- tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice și de comunicații;
- informează conducerea în caz de incidente, intervenție și rezolvarea incidentelor de securitate a informațiilor;
- asigură existența jurnalelor și a traseelor auditării pentru orice tip de acces în sistem conform procedurilor asociate;

- planifică, implementează și verifică zilnic soluțiile de securitate a informațiilor: server antivirus, firewall, server de actualizări de securitate, backup, acces securizat la camera severelor, asigurare aer condiționat, asigurare alimentare cu energie electrică/UPS;
- menține înregistrări privind configurația, aplicațiile și serviciile instalate, pentru a se putea reface sistemul în caz de dezastru;
- inventariază periodic aplicațiile și serviciile instalate și verifică dacă sunt autorizate;
- administrează sistemele IT și aplică măsurile de securitate și alte cerințe ale programului de securitate a informațiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

9.4. Utilizatorii datelor / sistemelor (angajați ARFCN, doctoranzi și terți care acționează într-o modalitate similară, cum ar fi furnizori de servicii, colaboratorii etc.):

- cunosc și respectă Planul de Securitate privind utilizarea Sistemului Informatic din cadrul Academiei Române Filiala Cluj-Napoca precum și procedurile și regulamentele aferente acestuia aplicabile pentru locurile lor de muncă,
- răspund direct de resursele informatice și de comunicații încredințate direct sau indirect,
- returnează echipamentele și informațiile încredințate în momentul încheierii relației contractuale sau în momentul solicitării returnării acestora de către ARFCN.

10. EXCEPȚII

Excepțiile de la regulile definite în aceast plan vor fi puse în aplicare numai după autorizarea prealabilă a Responsabilului IT, care va fi solicitată în scris și va include obligatoriu motivul excepției. Toate excepțiile vor fi considerate evenimente de securitate și vor fi comunicate Responsabilului IT și vor fi înregistrate în Registrul incidentelor de securitate, specificând data și ora, descrierea, motivul și modul de gestionare a riscurilor.

11. FORMULAR DE EVIDENȚĂ A MOFICĂRILOR

Nr. crt.	Numărul și data ediției	Numărul și data reviziei	Nr. pag. unde s-a efectuat modificarea	Descrierea modificării	Semnătura conducătorului compartimentului
1	Editia I din 21.07.2021	Rev 0	-		
2	Ediția II din _____	Rev 0	-		

12. FORMULAR DE ANALIZĂ A PROCEDURII

Nr. crt.	Compartiment/ institut	Conducător compartiment / institut/colectiv (Nume și prenume)	Înlocuitor de drept sau delegat	Aviz favorabil	Aviz nefavorabil			
				Semnătura	Data	Obs	Semnătura	Data
1.	Institutul de Lingvistică şi Istorie Literară "Sextil Puşcariu"							
2.	Biblioteca Academiei Române – Filiala Cluj-Napoca							
3.	Institutul de Istorie "George Barițiu – Departamentul de Istorie							
4.	Institutul de Istorie "George Barițiu" – Departamentul de Cercetări Socio-Umane							
5.	Centrul de Studii Transilvane							
6.	Arhiva de Folclor a Academiei Române							
7.	Institutul de Arheologie şi Istoria Artei							
8.	Centru de Cercetare Cluj							
9.	Institutul de Calcul „Tiberiu Popoviciu"							
10.	Observatorul Astronomic Cluj							
11.	Institutul de Speologie "Emil Racoviță" – ColectivulCluj							
12.	Institutul de Cercetări Socio-Umane din Tg. Mureș							

Anexa nr. 1

A1. Utilizarea permanentă a resurselor Informatice şi de Comunicaţii

Utilizatorul este responsabil de păstrarea în siguranță și folosirea corectă în scopurile destinate și autorizate a echipamentelor care i-au fost puse la dispoziție de ARFCN. Acestea includ stații de lucru fixe și mobile, imprimante, medii de stocare, telefoane mobile și fixe și alte mijloace de procesare a informațiilor, inclusiv software-ul asociat.

Reguli de utilizare permanentă a resurselor informatice şi de comunicaţii:

- ✓ Utilizarea Resurselor Informatice şi de Comunicaţii ARFCN se face numai în interes de serviciu;
- ✓ Utilizatorii trebuie să anunţe şeful ierarhic, RSSI şi DPO în cazul în care se observă orice problemă/breşă în sistemul de securitate a sistemului informatic din cadrul Academiei Române Filiala Cluj-Napocacât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare;
- ✓ 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 în cadrul sistemului informatic al Academiei Române Filiala Cluj-Napoca;
- ✓ Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din sistemul informatic pentru care nu au autorizaţie sau consimţământ explicit.

Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, numere de identificare personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau sau orice informaţii similare utilizate în scopuri de autorizare şi identificare;

- ✓ Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright);
- ✓ Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea Compartimentului IT/ Responsabilului IT, cu excepţia cazului în care acestea se găsesc incluse în lista programelor de tip shareware sau freeware utilizate în cadrul ARFCN (Anexa nr. 23 Lista programelor de tip shareware sau freeware) sau în lista programelor standard folosite în cadrul ARFCN (Anexa nr. 24 - Lista aplicaţiilor software permise a fi folosite în cadrul Academiei Române Filiala Cluj). Actualizarea acestor liste va fi realizată de către Compartimentul IT la propunerea responsabililor IT din cadrul Institutelor /Centrelor /Departamentelor ARFCN;
- ✓ Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele sistemului informatic; să împiedice accesul unui utilizator autorizat la sistemul informatic;
- ✓ Să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente;
- ✓ Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii sistemului informatic. De exemplu, utilizatorii ARFCN nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente;
- ✓ Sistemul informatic al Academiei Române Filiala Cluj **NU trebuie folosit pentru beneficiul personal**;
- ✓ Se interzice scoaterea informaţiei sau echipamentelor din sediul

ARFCN fără autorizarea/aprobarea şefului ierarhic şi/sau a conducerii ARFCN. În situaţia în care este necesară scoaterea informaţiei sau echipamentelor din sediu, se va face o solicitare scrisă prin care se va motiva/justifica necesitatea scoaterii informaţiei sau a echipamentelor;

- ✓ Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care ARFCN le poate considera ofensive, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea explicită a conducerii ARFCN);
- ✓ Accesul la reţeaua Internet prin intermediul sistemului informatic ARFCN se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru Utilizare Internet şi Intranet (Anexa nr. 8);
- ✓ Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la sistemului informatic al Academiei Române Filiala Cluj-Napoca;
- ✓ Utilizatorii care au acces la sistemul informatic al Academiei Române Filiala Cluj-Napoca au obligaţia de a purta acte şi/sau legitimaţii de serviciu care să ateste calitatea de utilizator autorizat în spaţiile ARFCN;
- ✓ Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Academiei Române Filiala Cluj-Napoca folosind resursele sistemului informatic;
- ✓ Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Academiei Române Filiala Cluj-Napoca sau prejudicierea, indiferent de formă, a intereselor ARFCN;
- ✓ Toate staţiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului (Lock prin apăsarea simultană a tastei Windows şi a tastei "L"), log off sau cu un screensaver protejat cu parolă, cu funcţia de activare automată setată la 5 minute sau mai puţin. La sfârşitul programului de lucru acestea, precum şi orice aparatură electrică şi electronică, trebuie să fie oprite;
- ✓ CD-urile, DVD-urile şi alte medii de stocare nu trebuiesc lăsate la vedere atunci când nu sunt folosite. Daca ele conţin date de maximă confidenţialitate, trebuie să fie ţinute sub cheie. CD-urile, DVD-urile, mediile de stocare mobile trebuie păstrate departe de acţiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui şi câmpuri magnetice;
- ✓ Toate mesajele, fişierele şi documentele localizate în cadrul SI-ARFCN sunt proprictatca Filialci şi pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor;

Anexa nr. 2

A2. Utilizarea ocazională a resurselor Informatice şi de Comunicaţii

În anumite situaţii este permisă utilizarea ocazională a sistemului informatic.
În aceste situaţii se aplică următoarele restricţii:

- ✓ 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.
- ✓ Utilizarea ocazională a sistemului informatic nu trebuie să aibă drept rezultate costuri directe pentru ARFCN.
- ✓ Utilizarea ocazională a sistemului informatic nu trebuie să afecteze activitatea normală a angajaţilor.
- ✓ 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.
- ✓ Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva ARFCN sau prejudicierea, indiferent de formă, a intereselor ARFCN.

Anexa nr. 3

A3. Reguli privind accesul fizic la resursele Informatice şi de Comunicaţii

- ✓ Toate sistemele de securitate fizică a Resurselor Informatice şi de Comunicaţii (RIC) – cum ar fi, de exemplu: coduri de acces în clădire şi coduri de acces pentru prevenirea incendiilor – trebuie să fie instalate în conformitate cu regulamentele ARFCN;
- ✓ Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat;
- ✓ Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate;
- ✓ Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic;
- ✓ Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea;
- ✓ Acordarea drepturilor de acces (folosind cartele, chei, parole etc.) se face de către conducătorul departamentului/institutului care deţine încăperea şi resursele;
- ✓ Nu este permis transferul dreptului de acces indiferent de motiv;
- ✓ Cartelele şi/sau cheile de acces care nu mai sunt folosite trebuie predate Compartimentului IT care le-a eliberat;
- ✓ Pierderea sau furtul cartelelor şi/sau cheilor de acces trebuie raportate imediat Compartimentului IT care le-a eliberat;
- ✓ Cartelele şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare;
- ✓ Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare încăpere şi, în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat;
- ✓ Fiecare Institut/Centru/Colectiv şi va ţine o evidenţă a tuturor cartelelor şi/sau cheilor de acces emise, retrase, pierdute sau furate;
- ✓ Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice;
- ✓ Fiecare Institut/Centru/Colectiv trebuie să verifice periodic drepturile de acces pe bază de cartelă şi/sau cheie şi să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces;
- ✓ Fiecare Institut/Centru/Colectiv trebuie să anuleze drepturile de acces ale cartelelor şi/sau cheilor utilizatorilor care îşi schimbă locul de muncă din ARFCN sau nu au relaţii contractuale cu ARFCN;
- ✓ Pentru fiecare spaţiu cu acces restricţionat trebuie desemnată o persoană care să verifice periodic înregistrările de acces şi să cerceteze orice acces suspect. Accesul restricţionat trebuie marcat.

Anexa nr. 4

A4. Reguli de acces la reţeaua de comunicaţii

✓ Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Compartimentul IT/ Responsabilul IT/ IIT;
✓ 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 şi datele de identificare ale acesteia se vor comunica către Responsabilul IT;
✓ Conectarea sistemelor de calcul care nu sunt proprietatea ARFCN se face numai cu aprobarea în scris a Compartimentul IT la recomandarea Institutelor sau departamentelor;
✓ Accesul de la distanţă la reţeaua ARFCN se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către ARFCN şi folosind protocoale aprobate de către IIT/Responsabilul IT;
✓ Utilizatorii din interiorul ARFCN nu se pot conecta la altă reţea;
✓ Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în niciun fel, pe nicio cale. Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv;
✓ Autorizarea tuturor conexiunilor se face la propunerea Institutelor/Centrelor/Colectivelor de către responsabilul IT;
✓ Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea responsabilului IT;
✓ Sistemele computerizate din afara ARFCN care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale ARFCN;
✓ Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii ARFCN nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua ARFCN;
✓ Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni;
✓ Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul IT/ Responsabilul IT;
✓ Serviciile de interconectare a reţelei ARFCN cu alte reţele sunt realizate exclusiv de către Compartimentul IT/ Responsabilul IT;
✓ Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Compartimetului IT. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate/acceptate de către Compartimentul IT/IIT.

Anexa nr. 5

A5. Regulament privind confidenţialitatea Serviciilor Informatice

✓ Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Academiei Române Filiala Cluj-Napoca, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament;

✓ Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Academiei Române Filiala Cluj-Napocapentru care nu au autorizaţie sau consimţământ explicit;

✓ Nici un utilizator al sistemului informatic al Academiei Române Filiala Cluj-Napocanu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului informatic. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu ARFCN;

✓ Confidenţialitatea informaţiilor transmise prin intermediul resurselor informatice ale terţilor nu poate fi asigurată/garantată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale al Academiei Române Filiala Cluj-Napoca se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora;

✓ În scopul administrării sistemului informatic, pentru asigurarea securităţii acestuia, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe/sau transportată prin sistemele informatice în conformitate cu legile în vigoare;

✓ Utilizatorii vor avea grijă să nu încalce drepturile de confidenţialitate ale altor persoane atunci când utilizează echipamentele (de exemplu, când fac înregistrări audio-video la locul de muncă);

✓ Utilizatorul trebuie să se asigure prin mijloace legale sau tehnice că informaţiile aparţinând sau aflate în custodia Academiei Române Filiala Cluj-Napoca rămân sub controlul ARFCN în orice moment;

✓ Stocarea de informaţii în interes de serviciu pe dispozitive aflate în afara controlului ARFCN, inclusiv pe dispozitive administrate de terţi cu care ARFCN nu are un acord contractual, este interzisă.

Anexa nr. 6

A6. Regulament de tratare a Incidentelor de Securitate

✓ Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor;
✓ RSSI este responsabil cu coordonarea pentru tratarea incidentului;
✓ RSSI este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului;
✓ RSSI este responsabil de coordonarea activităţilor de comunicare cu Compartimentul IT;
✓ Achiziţii pentru rezolvarea incidentului;
✓ În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare RSSI va recomanda sancţiuni disciplinare;
✓ În cazul în care incidentul implică aplicarea legilor civile sau penale DPO/RSSI va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu aceste.

Anexa nr. 7

A7. Regulament privind crearea şi utilizarea copiilor de siguranţă (Backup)

✓ Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor;
✓ Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul sistemului informatic trebuie să fie documentată şi periodic revizuită;
✓ Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile. Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă;
✓ 4. Benzile sau mediile utilizate pentru stocarea copiilor de siguranţă trebuie să aibă un sistem de identificare care să conţină cel puţin următoarele date de identificare a informaţiei stocate:

- numele sistemului;
- datele salvate;
- data creării copiei;
- numele persoanei care a efectuat copia de siguranţă (backup), informaţii de contact;

✓ Copiilor de siguranţă se vor crea şi utiliza de către fiecare conform procedurilor de sistem fiecărei Instituţii/Centre/Colective - Crearea copiilor de siguranţă (Backup);
✓ Furnizorul care oferă servicii de stocare a copiilor de siguranţă în alte zone pentru ARFCN trebuie să fie acreditat în acest scop de către o autoritate a statului;
✓ Procedurile stabilite între ARFCN şi furnizorii de stocare ale copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual;
✓ Accesul la mediile de backup ale ARFCN stocate la furnizori externi sau în interior se va face folosind card-urile sau proceduri specifice de acces. Acestea trebuie revizuite periodic (anual). Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă;
✓ Planul de recuperare în caz de dezastru al datelor şi informaţiilor se va întocmi la nivel de Institut/ Centre /Colective.

Anexa nr. 8

A8. Regulament de utilizare a reţelei Internet şi Intranet

✓ Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri academice şi de cercetare, în scopul desfăşurării activităţii specificate în fişa postului;
✓ Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către RSSI. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător;
✓ Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore;
✓ Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall;
✓ Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de Utilizare Permanentă a sistemului informatic (Anexa nr.1);
✓ Orice activitate a utilizatorilor folosind sistemului informatic poate fi înregistrată şi ulterior examinată;
✓ Conţinutul tuturor sit-urilor web ARFCN trebuie să se conformeze Regulamentelor de utilizare a SI şi să folosească numele de domeniu al Academiei Române Filiala Cluj-Napoca (acad-cj.ro);
✓ Nu se vor publica pe site-urile web al Academiei Române Filiala Cluj-Napoca materiale cu caracter ofensiv sau de hărţuire, materiale publicitare comerciale sau personale;
✓ Nu se vor publica pe sit-urile web ale ARFCN date ale instituţiei fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate;
✓ NU ESTE PERMISĂ UTILIZAREA SISTEMULUI INFORMATIC al Academiei Române Filiala Cluj-Napoca în scop personal sau pentru solicitări personale ce nu au legătură cu ARFCN;
✓ Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise;
✓ Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie al Academiei Române Filiala Cluj-Napoca;
✓ Orice material confidenţial al ARFCN transmis prin reţeaua Internet trebuie criptat/parolat;
✓ Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Institut/Centru/Colectiv;
✓ Utilizatorul care foloseşte Internetul, e-mail-ul sau resurse de pe Internet este obligat:

- să se asigure că toate comunicaţiile se fac în scopuri profesionale şi nu interferează cu productivitatea personal;
- să fie responsabili pentru conţinutul materialelor – text, imagine, audio sau de altă natură care plasează sau trimite pe Internet. Toate comunicaţiile vor avea ataşate numele angajatului;

✓ Angajatul este obligat să cunoască şi să respecte toate politicile şi procedurile asociate ale Academiei Române Filiala Cluj-Napocaşi de asemenea să păstreze secretul înregistrărilor la nivel personal sau de grup definit prin aceast plan.

✓ Angajaţilor ce utilizează Internetul şi/sau Intranetul nu le este permis să copieze, transfere, redenumească, adauge sau să şteargă informaţii sau programe ce aparţin altor persoane exceptând situaţia când li s-a permis acest lucru;

✓ 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.

Anexa nr. 9

A9. Regulament privind sistemul de Mesagerie Electronică

Adresa de e-mail instituțională furnizată de ARFCN şi mailbox-ul asociat acesteia, adresa IP şi, după caz, numărul de telefon fix, telefon mobil şi 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 şi nu introduce riscuri suplimentare pentru Filială.

Stocarea e-mail-urilor, documentelor şi altor fişiere personale nu este încurajată. În cazul în care acestea sunt totuşi păstrate, vor fi stocate local şi nu pe serverele ARFCN, în locaţii separate de cele care conţin informaţii ce aparţin Filialei. Toate mesajele şi fişierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Planul si Politica de Securitate a sistemului informatic din cadrul ARFCN.

ARFCN nu îşi asumă nicio responsabilitate cu privire la securitatea acestor informaţii, întreaga responsabilitate (inclusiv realizarea copiilor de siguranţă) revenind utilizatorului.

1. Următoarele activităţi sunt strict interzise utilizatorilor:

1.1. Trimiterea de mesaje cu caracter de intimidare sau hărţuire;

1.2. Folosirea sistemului de mesagerie electronică în scopuri personale;

1.3. Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;

1.4. Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate. Procurarea şi distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci şi logo-uri ale altor companii preluate din reviste, ziare, cărţi sau de pe internet);

1.5. Folosirea altei identităţi 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 identităţi de utilizator, pe orice mijloc de comunicare electronică, cu scopul de a induce în eroare destinatarul cu privire la identitatea expeditorului;

1.6. Utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităţilor ilegale, procurarea şi distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărţuire, defăimare sau ameninţare;

1.7. 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;

1.8. Transmiterea de informaţii confidenţiale sau secrete de serviciu altor destinatari decât cei autorizaţi să primească aceste informaţi;

1.9. Utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relaţii de afaceri care nu implică sau sunt contrare intereselor Academiei Română Filiala Cluj-Napoca din campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea Academiei Română Filiala Cluj-Napoca;

1.10. Postarea sau transmiterea de mesaje non-business identice sau similare către un număr mare de destinatari (news-group spam);

1.11. Utilizarca 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;

2. **Următoarele activități sunt interzise deoarece împiedică buna funcționare a comunicațiilor în rețea și eficiența sistemelor de mesagerie electronică:**
   2.1. Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția;
   2.2. Trimiterea mesajelor de dimensiuni foarte mari;
   2.3. Trimiterea sau retrimiterea mesajelor ce pot conține viruși.
3. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că își spun opinia sau dau declarații în numele Academiei Române Filiala Cluj-Napoca cu excepția situațiilor în care aceștia sunt autorizați în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declarație explicită prin care utilizatorul specifică faptul că nu reprezintă ARFCN. Un exemplu de declarație simplă este: "părerile exprimate sunt personale, și nu ale Academiei Române Filiala Cluj-Napoca... ".
4. Utilizatorii nu trebuie să 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.
5. 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".

Anexa nr. 10

A 10. Regulament de detectare a Viruşilor

✓ 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.

Anexa nr.11

A11. Regulament privind utilizarea dispozitivelor mobile

11.1 Reguli privind securitatea informaţiilor în cazul utilizării echipamentelor portabile de tip laptop

Regulile de utilizare a echipamentelor portabile de tip laptop sunt similare cu cele privind utilizarea staţiilor de lucru.

Suplimentar, având în vedere caracterul mobil al acestor dispozitive, ar trebui respectate următoarele reguli/ recomandări:

✓ Calculatoarele portabile trebuie să fie protejate prin parole;
✓ Se va evita stocarea datelor care privesc ARFCN pe dispozitivele portabile;
✓ În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc ARFCN trebuie criptate utilizând tehnici aprobate;
✓ Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţele sigure tip VPN, acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise;
✓ Toate accesările de la distanţă a Sistemului informatic ARFCN trebuie să se efectueze prin intermediul serviciului autorizat, conform Regulilor de acces la reţeaua de comunicaţii (Anexa nr. 4);
✓ Conectarea sistemelor de calcul care nu sunt proprietatea ARFCN se face numai cu acordul conducerii ARFCN, la recomandarea Institutelor /Centrelor/Colectivelor;
✓ Este recomandat să aveţi tot timpul controlul asupra laptop-urilor deoarece acestea pot fi ţinta unui atac dacă un atacator ar avea acces la ele. Dacă sunteţi nevoit să lăsaţi, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit şi să aibă discurile criptate. Sistemele de operare recente oferă nativ capabilitatea de criptare a

discurilor prin mecanisme proprii. Pentru versiuni mai vechi, dar şi pentru celelalte există produse care implementează acest serviciu. Astfel, puteţi evita accesul neautorizat la informaţii confidenţiale, în caz că laptop-ul este pierdut sau furat;

✓ În diverse locuri (cafenele, hoteluri, aeroporturi etc.) se găsesc hotspot-uri wireless sau chioşcuri care oferă servicii internet clienţilor.

Având în vedere că infrastructura ce deserveşte aceste reţele este una necunoscută şi că adeseori, securitatea nu e o preocupare în aceste locuri, există o serie de riscuri. Pentru a le contracara, iată câteva recomandări:

i. Dispozitivele mobile ar trebui să fie conectate la internet folosind reţelele 3G/4G, această modalitate fiind de preferat în locul hotspot-urilor WiFi;

ii. Dacă se foloseşte un hotspot Wi-Fi pentru accesul la internet, indiferent de reţeaua folosită, utilizatorii pot seta un tunel VPN către un furnizor de încredere pentru acest gen de servicii, protejând astfel tot traficul de date efectuat şi prevenind activităţi rău voitoare cum ar fi interceptarea traficului;

iii. Dezactivaţi funcţia "Network Share" înainte de a vă conecta la un hotspot public;

iv. Utilizaţi o aplicaţie firewall care să filtreze accesul din exterior;

v. Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa internetul, este recomandat să vă rezumaţi doar la navigarea pe web şi să evitaţi să accesaţi servicii unde trebuie să vă autentificaţi, deci să furnizaţi date de genul user/parolă;

v.1. Evitaţi să faceţi cumpărături online atunci când sunteţi conectaţi la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri. De obicei, informaţiile schimbate între dumneavoastră şi magazinul online, nu sunt criptate, şi pot fi interceptate uşor de către un atacator. În orice caz, dispozitivele utilizate pentru serviciu nu ar trebui utilizate pentru activităţi personale;

v.2. Nu folosiţi niciodată calculatoare publice pentru a efectua tranzacţii bancare, sau pentru alte tipuri de achiziţii online. Aceste calculatoare ar putea conţine programe care înregistrează datele personale, precum troienii bancari.

11.2 Reguli privind utilizarea echipamentelor portabile de tip tabletă şi smartphone

În afara casei, telefoanele mobile şi tabletele devin cele mai utilizate dispozitive electronice, iar provocările şi ameninţările asociate acestora sunt diferite şi necesită o abordare specială. Principalele probleme care pot apărea, sunt furtul sau pierderea dispozitivelor, descărcarea de aplicaţii ce conţin viruşi, fură informaţii sensibile şi direcţionează utilizatorii către site-uri şi documente compromise.

Următoarele reguli vor contribui la reducerea riscurilor:

1. Asiguraţi-vă că toate software-urile sunt actualizate. Actualizaţi-vă sistemele de operare pentru dispozitivele mobile. Dispozitivele mobile trebuie tratate ca şi computerele personale în sensul că toate software-urile de pe dispozitive trebuie actualizate, în special software-urile de securitate. Acest lucru va proteja dispozitivele împotriva noilor versiuni ale software-urilor rău intenţionate şi a viruşilor care ameninţă informaţiile critice ale organizaţiei.

Este recomandat să faceţi acest lucru atunci când apar versiuni noi şi să verificaţi acest lucru periodic. Sunteţi mult mai vulnerabili atunci când utilizaţi dispozitivele mobile (telefon, tabletă etc.) în timpul unor călătorii, deoarece ameninţările, sunt probabil mai prezente în reţelele publice din aeroporturi, gări, obiective turistice etc.

2. Protejați-vă terminalul cu parole. În cazul în care cineva vă fură sau vă găsește telefonul/tableta, îngreunați-i accesul la informațiile stocate. Pe lângă criptare și actualizările de securitate, este importantă utilizarea parolelor puternice pentru a proteja datele stocate pe dispozitivele mobile. Acest lucru va ajuta la împiedicarea accesării datelor sensibile în caz că dispozitivul este pierdut sau ajunge în mâinile hackerilor.
3. Criptați datele de pe dispozitivele mobile. Informațiile de afaceri și personale stocate pe dispozitivele mobile sunt adesea sensibile. Criptarea acestor date reprezintă o necesitate. Dacă un dispozitiv este pierdut și cartela SIM furată, hoțul nu va putea accesa datele dacă pe dispozitiv este încărcată tehnologia corespunzătoare de criptare.
4. Utilizați software-uri de securitate pe toate telefoanele inteligente. Software-urile de securitate concepute special pentru telefoanele inteligente pot opri hackerii și împiedica infractorii cibernetici să vă fure informațiile sau să vă spioneze atunci când utilizați rețelele publice. Acestea pot detecta și elimina viruși și alte amenințări mobile înainte să vă cauzeze probleme. Acestea pot de asemenea să elimine textul supărător și mesajele spam multimedia.

   Folosiți o soluție de securitate care să aibă un modul antifurt, în mod special dacă folosiți un echipament care rulează Android. Din cauza cotei de piață ridicate, telefoanele/tabletele bazate pe Android au devenit ținta predilectă a infractorilor informatici.

   Alegeți însă o sursă reputată și urmăriți furnizorii care oferă și soluții de securitate pentru PC pentru a evita soluțiile de securitate false. O soluție antivirus vă permite să filtrați aplicațiile potențial periculoase și să le blocheze înainte ca acestea să cauzeze modificări asupra sistemului. În cazul în care pierdeți echipamentul sau vă este furat, modulul antifurt vă poate ajuta să identificați și să îl recuperați. De asemenea acesta poate fi utilizat pentru a bloca echipamentul sau pentru a șterge informațiile de pe el de la distanță. În cazul telefonului aceste operații pot fi efectuate chiar dacă acesta nu are acces la internet, un simplu SMS putând fi utilizat pentru blocarea acestuia sau pentru ștergerea informațiilor personale;
5. Sincronizați-vă telefonul/tableta cu un calculator personal. În cazul în care pierdeți aceste echipamente sau vă sunt furate, veți avea o copie de siguranță a contactelor, mesajelor, imaginilor și documentelor stocate pe acestea;
6. Accesați doar hotspot-uri sigure. Asigurați-vă că opțiunile de conexiune prin infraroșu, Wi-Fi și Bluetooth-ul sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil;
7. Fiți atenți ce aplicații descărcați și de unde. Să fie descărcate numai din magazinele oficiale ale operatorilor și producătorilor precum Google Play, Apple App Store sau Microsoft Store.

   Soft-urile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta și pot trimite mai departe, unor terțe părți informații private. În zone necunoscute, ați putea fi tentați să descărcați aplicații care să vă ajute să găsiți diferite locații precum restaurante, hoteluri sau muzee. Aveți însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea din greșeală a aplicațiilor nesigure, verificați configurația terminalului accesând SETĂRI, SECURITATE și asigurându-vă că opțiunea SURSE NECUNOSCUTE este nebifată.
8. Fiți atenți la ofertele prea bune pentru a fi reale. Dacă primiți dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la prețuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignorați-le. Un click pe link-urile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completați formulare cu informații personale.

Nu uitaţi de asemenea că telefonul/tableta dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website;

9. Când folosiţi reţelele sociale, asiguraţi-vă că fotografiile făcute cu smartphone-ul şi pe care doriţi să le încărcaţi pentru a le partaja cu prietenii, nu conţin informaţii legate de poziţia dumneavoastră actuală. Partajarea locaţiei e ideală pentru întâlnirile cu amicii în locuri publice, dar în acelaşi timp, permit persoanelor rău-intenţionate să vă monitorizeze obiceiurile şi rutina zilnică facilitând tentativele de hărţuire;
10. Aveţi mare grijă la ce fotografiaţi. Puteţi fi tentat să fotografiaţi şi să procesaţi coduri QR (coduri de bare care stochează informaţii despre diverse produse sau linkuri către website-uri). Dacă fotografierea şi procesarea codurilor QR de pe ambalajele produselor nu sunt, de obicei, periculoase, puteţi găsi coduri QR lipite în locuri publice sau chiar desenate pe elemente de mobilier stradal, ziduri etc. Aceste coduri pot conţine URL-uri către website-uri care să exploateze vulnerabilităţi din telefonul dumneavoastră care să se finalizeze cu o infecţie.
11. Utilizatorii să fie conştienţi de împrejurimi. Fie că introduc parole sau vizualizează date sensibile sau confidenţiale, utilizatorii trebuie să fie precauţi la cei care se pot uita peste umărul lor.
12. Utilizaţi aceste strategii pentru email, transmiterea mesajelor şi reţelele de socializare:
    - ✓ Evitaţi deschiderea mesajelor text neaşteptate din partea expeditorilor necunoscuţi– ca şi în cazul emailului, atacatorii pot utiliza mesaje text pentru a răspândi software-uri rău intenţionate, înşelătorii de tip phishing şi alte ameninţări printre utilizatorii de dispositive mobile. Aceeaşi precauţie trebuie aplicată pentru deschiderea mesajelor text nesolicitate cu care utilizatorii s-au obişnuit în cazul emailului;
    - ✓ Nu vă lăsaţi ademeniţi de spammeri şi phisheri. Pentru a proteja reţelele organizaţiei împotriva infractorilor cibernetici, ar trebui să implementaţi soluţii corespunzătoare de securitate a emailurilor, inclusiv prevenirea spamurilor. Astfel puteţi proteja reputaţia şi gestiona mai precis riscurile;
    - ✓ Daţi click cu precauţie. Exact ca pe computerele staţionare, comunicarea pe reţelele de socializare pe dispozitivele mobile şi laptopuri trebuie realizată cu grijă şi precauţie. Utilizatorii nu trebuie să deschidă linkuri neidentificate. Nu durează mult ca un utilizator să fie păcălit să compromită un dispozitiv şi informaţiile de pe acesta;
13. Asiguraţi-vă că toate dispozitivele sunt curate înainte de aruncare. Majoritatea dispozitivelor mobile au o funcţie de resetare care permite ca toate datele să fie şterse. Cartelele SIM trebuie, de asemenea, să fie şterse şi distruse.

Anexa nr. 12

A 12. Regulament privind parolele de acces

Parola de acces este proprietatea personală a utilizatorului final, care va fi obligat să respecte următoarele reguli:

- Orice parolă ar trebui să fie complexă şi să aibă o lungime minimă de 8 caractere.

O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#+-&^* ...).

Criterii pentru stabilirea unei parole:

- nu este deloc recomandată folosirea simplă a datelor personale (ex: data naşterii, nume, prenume etc.) ca parole.
- folosiţi cifre şi simboluri uşor de asociat prin forma lor cu litere. De exemplu: a=@ B=8, E=3, i=1, I=!, O=0(zero), s=$.

Exemple:

Aşa nu	Aşa da
maria1974	#p0p3$cu#!974
petrea	m4m&

- faceţi asocieri dupa ceva ce vă place: o carte, titlul unei melodii, titlul unui film, personajele dintr-un film etc. şi trasaţi-vă nişte reguli de formare a parolei pe care sa le folosiţi de fiecare dată când aveţi nevoie de o parolă nouă.

De exemplu: Prin asocierea iniţialelor (să hotărâm că le vom folosi ca litere minuscule) titlului filmului „Pulp fiction" cu primele două litere din numele şi prenumele personajelor Vincent Vega şi Mia Wallace, folosind cifre şi simboluri uşor de asociat cu litere (i=1, e=3, a=@), se poate obţine parola: pfV1V3M1W@. Nu trebuie să vă străduiţi foarte mult să ţineţi minte această parolă - care pare a fi complicată la prima vedere - pentru ca o puteţi deduce logic de fiecare dată când aveţi nevoie de ea, important e sa ţineţi minte regulile după care aţi format-o.

- Nu va folosi aceeaşi parolă pentru mai multe conturi;
- Nu va afişa parola de acces prin scriere/tipărire pe hârtie sau post-it sau alte asemenea suporturi;
- Nu va transmite parola de acces altor persoane, inclusiv colegilor de birou, chiar dacă aceştia se oferă să îi ajute în utilizarea staţiei de lucru;
- Înainte de plecarea din sediu pentru perioade mai mari de timp (delegaţii, concedii etc.) va pune la dispoziţia colegilor săi datele care le-ar putea fi necesare pentru buna desfăşurare a activităţii, astfel încât aceştia să nu aibă nevoie ulterior de parola sa de acces;
- Dacă trebuie să lucreze pe o altă staţie decât cea pentru care este responsabil, el va folosi propriul nume de utilizator (user name) şi parola de acces (password) proprie pentru a accesa această staţie, dacă aceasta este într-un domeniu; în caz contrar, administratorul de reţea va crea un nou cont pentru acel utilizator;
- Nu va încerca să anuleze parolele de acces pentru bios, dacă acestea există;
- Asigură protejarea accesului la date prin blocarea staţiei de lucru ori de câte ori este obligat să se deplaseze de lângă aceasta;
- Este singurul răspunzător de confidenţialitatea parolei de acces, aceasta fiind mijlocul de autentificare şi prima barieră în cazul unei tentative de acces neautorizat la resurse;
- Dacă aveţi multe parole le puteţi scrie într-un fişier, însă criptaţi acel fişier şi asiguraţi-vă că nu-l veţi pierde. Evitaţi denumirea acelui fişier cu una explicită (parolelemele.zip);

- Evitaţi să pastraţi parole în agende electronice, telefoane mobile – pot fi furate;
- Parolele trebuie să fie schimbate de utilizator în mod regulat, cel puţin o dată la 3 luni;
- Aveţi grijă la facilitatea browser-elor de reţinere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucraţi e folosit de mai multe personae;
- Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice;
- Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat;
- Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrative;
- Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă;
- **Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:**
  - utilizatorul se va legitima ;
  - administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
  - utilizatorul va introduce o nouă parolă.
- Responsabilii IT au în responsabilitate atribuţii cu competenţe de verificare a schimbării periodice a parolelor de acces

Identificare şi autentificare

- Utilizatorul este responsabil pentru securitatea datelor, a informaţiilor de autentificare şi a sistemelor aflate sub controlul său;
- Utilizatorul trebuie să păstreze credenţialele de acces (nume utilizator, parolă, token etc.) în siguranţă şi să nu le împărtăşească nici unei alte persoane, inclusiv colegi, membri ai familiei sau prieteni;
- Asigurarea accesului altei persoane, fie în mod deliberat, fie prin incapacitatea de a păstra în siguranţă informaţiile de autentificare, reprezintă o încălcare a acestui plan;
- Nici un angajat ARFCN nu trebuie, sub nici o formă, să acceseze neautorizat sau să permită accesul neautorizat la informaţiile, fişierele, calculatoarele sau alte dispozitive din reţeaua Academiei Română Filiala Cluj-Napoca. Acesta este considerat caz de fraudă majoră;
- La părăsirea calculatorului trebuie ca utilizatorul să iasă din reţea (log off);
- **De asemenea sunt interzise**:
  - încercarea utilizatorilor de a vizualiza şi deduce parolele altora în timpul introducerii acestora;
  - transmiterea de parole în clar prin intermediul sistemelor de comunicaţii (e-mail, mesagerie instant, SMS etc.);
  - afişarea conturilor sau parolelor de acces la echipamente sau sistem informatic.
- Toate staţiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Astfel, la părăsirea calculatorului/ aplicaţiei folosite, fiecare utilizator trebuie să aplice măsuri precum blocarea sau închiderea echipamentului şi blocarea sau închiderea aplicaţiei utilizate în funcţie de: durata de timp până la următoarea utilizare a echipamentului sau aplicaţiei, de securizarea zonei în care este poziţionat echipamentul, de folosirea în comun de către mai multe persoane a spaţiului în care este poziţionat echipamentul, de folosirea în comun de către mai multe persoane a echipamentului şi aplicaţiilor.

Anexa nr. 13

A 13. Regulament privind crearea şi administrarea conturilor

Personalul care asigură suport tehnic, administratorii de sistem, responsabilii IT şi alte persoane pot avea conturi cu drepturi de acces privilegiat în comparaţie cu utilizatorii obişnuiţi. Datorită faptului că aceste conturi pentru acces administrativ au mai multe privilegii, aprobarea, verificarea şi monitorizarea acestora sunt extrem de importante din punctul de vedere al securităţii SI.

- Accesul la sistem este permis doar personalului autorizat şi identificat în mod unic
- (utilizatori/users);
- Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare;
- Toate conturile de acces se vor crea în formatul standard cont utilizator prenume.nume sau nume.prenume;
- Prin contractul de muncă şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului informatic;
- Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces;
- Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat;
- Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu regulamentul privind parolele de acces;
- Toate conturile utilizator care nu au fost accesate timp de 90 de zile vor fi dezactivate;
- După încă 90 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea;
- Responsabilul IT trebuie să aibă o documentaţie de modificare a conturilor de utilizator pentru situaţii precum schimbări ale numelor de familie, modificări privind contul (numele contului), modificări ale drepturilor de utilizator;
- Institutele şi/sau Centrele/Colectivele ARFCN, prin responsabilii IT desemnaţi, trebuie să prezinte la Compartimentul IT o listă cu informaţii în plan administrativ pentru toate sistemele conectate la reţeaua de comunicaţii a Filialei Cluj- Napoca a Academiei Române. Această listă trebuie refăcută şi prezentată la Compartimentul IT anual sau de fiecare dată când apar modificări de orice natură.

Anexa nr. 14

A 14. Securitatea echipamentelor şi resurselor în afara locaţiei ARFCN

Folosirea echipamentelor în afara locaţiei ARFCN creşte riscurile de securitate ale acestora, echipamentele fiind în special vulnerabile la daune fizice, pierdere şi furt. În acest caz, se vor aplica următoarele măsuri de securitate:

- Echipamentul va fi instalat conform regulamentelor ARFCN şi a legislaţiei în vigoare;
- În momentul părăsirii ARFCN, echipamentul poate fi utilizat pentru resursele online (ex. e-mail) şi va exista acces la informaţiile statice;
- Update-urile aplicaţiilor (de exemplu: sistem de operare, antivirus, Suita Office etc.) se vor face doar la revenirea cu echipamentul în reţeaua Academiei Române Filiala Cluj-Napoca-Napoca. Utilizatorul are obligaţia ca la un interval de maximum 4 săptămâni să introducă echipamentul în reţeaua internă a ARFCN pentru actualizări ;
- Accesul la aplicaţiile de pe serverele ARFCN (de ex. iConsalt, ESA4, Legis Reţea) se va face doar de la sediul ARFCN;
- Documentele personale (valabil pentru toate echipamentele) se vor ţine într-un folder
- "Personal".
- Furtul sau pierderea unui echipament scos în afara ARFCN vor fi raportate imediat şefului ierarhic.

Detalii suplimentare în *Anexa nr. 11- Regulament privind utilizarea dispozitivelor mobile*

Anexa nr. 15

A 15. Utilizarea echipamentelor proprietate personală

- ARFCN poate permite angajaților sau persoanelor terțe să folosească echipamente proprietate personală (EPP) pentru îndeplinirea sarcinilor de serviciu;

Următoarele echipamente proprietate personală sunt permise:

- dispozitive de tip smartphone având sisteme de operare: iOS, Android, Blackberry sau Windows;
- tablete având sisteme de operare: iOS, Android, Windows;
- laptop-uri;
- dispozitive de stocare portabile: stick-uri de memorie USB, carduri de memorie, hard-disk-uri portabile etc.

- **Utilizarea echipamentelor proprietate personală este asociată cu o serie de riscuri de securitate a informațiilor, cum ar fi:**
  - pierderea, dezvăluirea sau alterarea informațiilor Academiei Române Filiala Cluj –Napoca stocate pe EPP;
  - incidente care implică amenințări la adresa infrastructurii informatice a Filialei sau compromiterea acestei infrastructuri (de exemplu: viruși, malware, hacking);
  - nerespectarea legilor, reglementărilor și obligațiilor contractuale (de exemplu, protecția datelor cu caracter personal, legislația anti-piraterie etc.);
  - nerespectarea drepturilor de proprietate intelectuală pentru informațiile ARFCN create, stocate, procesate sau transmise pe EPP.
- Angajații care folosesc EPP pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizați în mod explicit să facă acest lucru. Autorizarea va fi dată de responsabilul IT la cererea șefului direct ca răspuns la o solicitare în care este explicat motivul solicitării;
- Utilizatorii trebuie să asigure aceleași măsuri de protecție a informațiilor ca și cele aplicate pentru echipamentele ARFCN și nu trebuie să introducă riscuri inacceptabile (exemplu: malware) în rețeaua filialei prin utilizarea de echipamente nesigure;
- Academiei Române Filiala Cluj-Napoca își rezervă dreptul de a refuza sau de a retrage autorizarea în cazul în care consideră că echipamentul nu este adecvat și/sau nu este folosit în interesul ARFCN;
- În timp ce utilizatorii au o așteptare rezonabilă de intimitate asupra informațiilor lor personale pe propriul echipament, dreptul ARFCN de a controla propriile date și de a gestiona EPP poate duce ocazional la accesul neintenționat al personalului de asistență la informațiile lor personale. Pentru a reduce posibilitatea unui astfel de acces, utilizatorii trebuie să păstreze datele lor personale separat de datele ARFCN, în directoare separate, denumite în mod sugestiv.

Anexa nr. 16

A 16. Regulament de acces la distanță

- Accesul de la distanță la rețeaua ARFCN se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către ARFCN și folosind protocoale aprobate de către IIT/Responsabilul IT.;
- Toate accesările de la distanță a Sistemului informatic ARFCN trebuie să se efectueze prin intermediul serviciului autorizat, conform Regulilor de acces la rețeaua de comunicații (Anexa nr. 4).;
- Accesul de la distanță la rețeaua și resursele ARFCN trebuie să utilizeze tehnologia VPN (Virtual Private Network). Trebuie să existe implementat un mecanism puternic de autentificare și criptare;
- Accesul se va acorda numai pentru îndeplinirea atribuțiilor de serviciu;
- Accesul în anumite aplicații este permis numai folosind desktop-uri virtuale;
- Se vor folosi doar dispozitive și software furnizat sau acceptat de ARFCN;
- Pentru comunicarea și colaborarea cu colegii, pentru ședințe este necesară o soluție de videoconferință, pentru lucrul colaborativ, respectiv accesarea resurselor ARFCN trebuie avute în vedere partajarea documentelor în cloud, conexiunea la rețeaua instituției (VPN), accesul la serverele de fișiere interne și e-mail-ul ca alternativă iar protecția datelor pe stațiile de lucru se asigură prin discuri criptate pentru salvarea informațiilor;
- Finalizarea deciziilor se poate face prin utilizarea semnăturii electronice calificate bazate pe un certificat digital calificat;
- Creați parole puternice, nu le scrieți și protejați-le atunci cînd le tastați;
- Înainte de a începe lucrul de la distanță, familiarizați-vă cu dispozitivele, politicile și procedurile ARFCN! Asigurați-vă că înțelegeți modul de operare al echipamentelor, ceea ce trebuie făcut și ce nu în cazul acestora, dar și unde să vă adresați în cazul apariției unor probleme;
- Conectați-vă la rețeaua ARFCN doar prin VPN și protejați token-urile (sau cardurile inteligente) necesare pentru conexiunea VPN.;
- Nu permiteți membrilor familiei sau altor persoane să vă acceseze dispozitivele de lucru!
- Blocați-le sau închideți-le când sunt nesupravegheate și păstrați-le întotdeauna într-o locație sigură, pentru a preveni pierderea, deteriorarea sau furtul. Împiedicați scurgerea de date accidentală, folosind ecrane de protecție a confidențialității și evitați orientarea ecranelor spre ferestre sau camere foto;
- Dacă observați vreo activitate neobișnuită sau suspectă, pe orice dispozitiv pe care îl utilizați pentru a lucra la distanță, contactați imediat angajatorul pe canale de comunicare sigure;
- Atenție la orice activități sau cereri suspecte, în special la cele financiare. Ar putea fi o fraudă! În cazul în care aveți dubii, apelați solicitantul pentru a verifica. Nu faceți clic pe linkurile sau fișierele atașate primite în e-mailuri și mesaje text nesolicitate;
- Nu răspundeți niciodată cu informații personale la mesaje, chiar dacă pretind că provin dintr-o afacere legitimă. În schimb, contactați direct compania pentru a confirma solicitarea acestora;
- Discutați planurile de lucru cu conducerea și membrii echipei, în perioada lucrului de la distanță, inclusiv distribuirea sarcinilor, a termenelor și a canalelor de comunicare;

- ❖ Dacă utilizarea dispozitivului personal este singura opțiune de lucru și angajatorul dvs. vă permite folosirea lui, asigurați-vă că sistemul de operare și software-ul dispozitivului sunt actualizate, aveți o soluție antivirus instalată, iar conexiunea este securizată printr-un VPN aprobat;
- ❖ Este interzisă transmiterea documentelor prin aplicații de mesagerie (Facebook ,Messenger, Whatsapp) sau încărcarea lor pe site-uri publice de transfer de fișiere;
- ❖ Evitați folosirea în interes personal a dispozitivelor dedicate lucrului de la distanță!

Măsuri pentru securizarea mediului de lucru de la distanță:

a. Schimbați numele de utilizator şi parola implicită a routerului wifi;
b. Instalați o soluție antivirus pe dispozitivele utilizate pentru lucrul la distanță;
c. Revizuiți permisiunile aplicațiilor la date și dezactivați-le acolo unde nu este necesar accesul;
d. Alegeți parole puternice, complexe, în special în cazul conturilor de e-mail Efectuați back-up regulat al datelor esențiale;
e. Actualizați automat software-ul de pe dispozitive. Astfel de măsuri scad riscul de compromitere a dispozitivelor prin vulnerabilități nerezolvate;
f. Securizați dispozitivele electronice cu parole, coduri PIN sau informații biometrice (amprentă, Face ID, etc);
g. Revizuiți setările de privacy ale conturilor de social media.

Anexa nr. 17

A17. Politica biroului curat şi a ecranului curat

1. Pentru a minimiza posibilitatea pierderii de date, a furtului sau a dezvăluirii neautorizate, personalul ARFCN trebuie să adopte practici conştiente de securitate la locul de muncă. Acest lucru necesită blocarea tuturor datelor sensibile asupra materialelor fizice atunci când nu sunt utilizate (politica biroului curat).
2. Toţi utilizatorii din cadrul ARFCN trebuie să ia în considerare adoptarea unei "politici de birou curat" atât pentru documentele pe suport tip hârtie, cât şi pentru medii/suporturi externe de stocare a datelor. De asemenea, trebuie adoptată politica "ecranului curat" pentru echipamentele de procesare a informaţiei, în scopul reducerii riscului de acces neautorizat, precum şi de pierdere sau distrugere a informaţiei în timpul sau în afara orelor de lucru normale.
3. Această politică trebuie să ţină seama de clasificările de securitate ale informaţiei, precum şi de riscurile aferente.
4. Acolo unde se consideră necesar, documentele pe suport tip hârtie şi mediile/suporturile externe de stocare a datelor trebuie păstrate în dulapuri încuiate şi/sau în alte tipuri de mobilier securizat, atunci când nu sunt folosite, mai ales în afara programului de lucru.
5. În afara programului normal de lucru, imprimantele şi scanerele trebuie protejate faţă de accesul neautorizat.
6. Informaţiile confidenţiale sau clasificate, după ce sunt imprimate, trebuie ridicate imediat din imprimantă.
7. Se va evita încărcarea inutilă a spaţiului rezervat pe staţia de lucru, pe servere şi în sistemul de poştă electronică cu fişiere multimedia de mari dimensiuni şi se va proceda la ştergerea periodică a informaţiilor perimate.
8. Toate calculatoarele trebuie inchise inainte de sfarsitul zilei de lucru
9. La finalul programului de lucru, laptopurile trebuie încuiate într-o camera dedicata/sertar cu cheie sau blocate prin utilizarea unui cablu de securitate.
10. Atunci cand o statie de lucru nu este utilizata aceasta trebuie sa fie închisă.
11. Statiile de lucru pentru calculatoare trebuie inchise complet la sfarsitul zilei de lucru.
12. Utilizatorii trebuie să presupună că locul de muncă poate fi accesat de către persoane din afară. Prin urmare, personalul ARFCN nu trebuie sa-şi părăsească terminalul conectat şi nesupravegheat, trebuie să aleagă parole nontriviale şi să le păstreze în siguranţă
13. Toate staţiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului (Lock prin apăsarea simultană a tastelor ***Windows*** + ***L***), log off sau cu un screensaver protejat cu parolă, cu funcţia de activare automată setată la 5 minute sau mai puţin.

Anexa nr. 18

A18. Securitatea fizică a echipamentelor IT

Datorită importanţei lor deosebite, componentele sistemelor electronice de calcul trebuie să beneficieze de un tratament aparte.

Se ştie că o cale sigură de compromitere a securităţii unui sistem electronic de calcul este de natură fizică, modificându-i anumite elemente din configuraţie astfel încât, faţă de configurarea dată de utilizator, să se creeze căi de acces pentru cei rău intenţionaţi sau să se blocheze mijloacele de asigurare a securităţii sistemului. În acest sens, se pot modifica circuitele electronice, se pot adăuga mici „şmecherii" (circuite cu rol special, emiţătoare, microfoane), se pot realiza derivaţii ale canalelor de comunicaţie, pot fi scurt-circuitate componentele cu rol de protecţie, citirea pe ascuns a memoriei în care sunt păstrate parolele sistemului, scoaterea controlului existent pe terminale pentru depistarea pătrunderilor neautorizate.

Echipamentele, în pofida reclamei făcute de producători, sunt predispuse la căderi, fie datorită unor defecţiuni de fabricaţie, fie instalării greşite, fie datorită defectării în timpul transportului. Dar, cel mai grav, echipamentele pot „cădea" în timpul exploatării lor, devenind atât ele, cât şi datele conţinute în memorie inutilizabile. Uneori şi softul cu care se lucrează poate fi pierdut.

Sunt dese cazurile când echipamentele nu au certificat de origine, fie în întregime, fie numai pentru unele dintre miile de componente din structura lor. Incertitudinea aplanează asupra a ceea ce s-a cumpărat şi consecinţele sunt şi mai grave atunci când distribuitorul este un ilustru necunoscut.

Întreţinerea sau depanarea sistemului sunt asigurate, de regulă, de specialişti din afară. Cu multă uşurinţă ei pot realiza toate operaţiunile menţionate anterior pentru paralizarea sistemului.

Apărarea împotriva tuturor pericolelor descrise are un rol vital în buna funcţionare a sistemului. Totuşi, trebuie pornit de la faptul că toate componentele sistemelor, la rândul lor, pot dispune de elemente proprii de asigurare a securităţii.

18.1 Asigurarea echipamentelor împotriva intenţiilor de modificare a lor

Toate componentele sistemelor de prelucrare automată a datelor trebuie protejate, fie împotriva hoţilor, fie a vandalilor. Sunt unele elemente care necesită însă o grijă deosebită. De exemplu, terminalele nu sunt la fel de importante ca şi calculatorul central sau serverele sistemului.

Echipamentele pot fi protejate împotriva modificării lor astfel:

- Birourile ce conţin hardware trebuie să fie încuiate, sigilate cu benzi de hârtie sau cu plumb. Sigiliile vor fi verificate periodic pentru depistarea accesului neautorizat. Cele mai moderne sigilii sunt cele holografice care conţin imagini unice, imposibil de recreat.
- Echipamentele trebuie să fie, pe cât posibil, mai dispersate, îndeosebi în cazul lucrului cu informaţii speciale.
- Elementele din configuraţia fizică a sistemului care sunt deosebit de importante, cum ar fi cazul plăcii cu circuite, pot fi fotografiate la intervale regulate de timp pentru a compara fotografiile mai multor perioade în vederea depistării eventualelor modificări.

Este posibil ca fiecare echipament periferic să aibă atribuit un număr unic de identificare, interpretabil de către calculator la deschiderea sesiunii de lucru şi confirmat ulterior când se solicită o operaţiune la/de la perifericul respectiv. Fiecare imprimantă, terminal sau legătură din reţea trebuie să aibă definite categoriile de informaţii cu care pot lucra sau funcţiile din sistem ce se realizează prin intermediul lor. Numerele unice de identificare înlesnesc tratarea diferenţiată a perifericelor sau a celorlalte componente. De exemplu, terminalele amplasate în diverse locuri din unitate, pentru a veni în sprijinul oricărui utilizator comun al firmei, nu trebuie să aibă şi dreptul de accesare a sistemului de operare al calculatorului central sau să restaureze date în scopul manipulării lor. De asemenea, imprimantele din diverse birouri nu pot folosi datele secret care au un regim sever la tipărire.

O măsură suplimentară de control va consta în stabilirea momentelor din zi când un echipament periferic sau un utilizator a accesat sistemul. Oricum nu este recomandat să se permită angajaţilor firmei să lucreze peste program, iar când aceasta se impune va fi sub un control riguros.

18.2 Controlul integrităţii echipamentelor

Calculatoarele pot să-şi verifice singure starea în care se află celelalte componente, prin autodiagnoză, astfel încât să poată descoperi ce nu funcţionează cum trebuie. Printre activităţile realizate de calculatoare vor fi verificarea modului de lucru, inclusiv urmărirea funcţiilor de realizare a securităţii sistemului, precum şi facilităţile de control al accesului.

Autodiagnoza este utilă pentru:

- confirmarea cu precizie a identităţii echipamentelor, suporturilor şi utilizatorilor
- elementele de bază ale sistemului;

verificarea dacă utilizatorii folosesc doar echipamentele, softul şi datele la care ei au acces de drept şi preîntâmpinarea accesului neautorizat;

- asigurarea că orice tentativă de acces sau utilizare neautorizată a

echipamentelor, softului sau datelor este blocată şi că supraveghetorii sistemului vor fi anunţaţi imediat.

Simpla realizare a funcţiilor de mai sus nu înseamnă neapărat şi perfecţiunea sistemului de securitate, dar constituie suficiente măsuri de apărare a sistemului împotriva atacurilor rău intenţionate.

Există şi producători de calculatoare care asigură facilităţi de diagnoză de la distanţă a stării sistemului, ceea ce în mod normal se realizează de către echipele de service, pentru a se asigura că totul funcţionează corect şi că nu se conturează posibilitatea apariţiei unor defecţiuni.

Astfel de metodă este benefică pentru unitate, întrucât duce la reducerea costurilor şi se realizează mult mai rapid decât în varianta apelării la inginerii de întreţinere. Totuşi, diagnoza de la distanţă este destul de periculoasă pentru securitatea sistemului, intruşilor oferindu-li-se o şansă în plus să acceseze orice element din configuraţie, aceştia având la dispoziţie o linie specializată. Aşadar, aparentul cost redus poate să însemne pierderi mult mai mari.

18.3 Proceduri de întreţinere a echipamentelor

Activităţile de întreţinere şi reparare a oricărui echipament pot genera o mulţime de semne de întrebare privind siguranţa, securitatea şi disponibilitatea datelor din sistem. Din această cauză este foarte important să se controleze accesul la echipamente şi software şi să se supravegheze îndeaproape specialiştii care asigură întreţinerea sau repararea sistemului.

O primă măsură va consta în deschiderea unui registru de întreţinere, în care să se înregistreze toate detaliile privind o astfel de activitate. Ele se vor referi la data şi timpul efectuării lor, numele tehnicienilor, motivul vizitei lor, acţiunile şi reparaţiile ce au avut loc, inclusiv componentele hard care au fost adăugate, reparate, înlocuite sau reînnoite. Fiecare înregistrare din registru va fi contrasemnată de responsabilul cu securitatea sistemului. Registrul trebuie să fie consultat periodic pentru descoperirea eventualelor nereguli.

Ca şi în cazul diagnozei de la distanţă, în timpul întreţinerii sau reparării sistemului trebuie să fie scoase datele şi softul de pe benzi sau pe discuri de orice tip, iar cele din memoria principală, de asemenea, salvate, reiniţializându-se sistemul numai în acest scop. Specialiştilor ce efectuează întreţinerea nu trebuie să li se înlesnească accesul la datele speciale ale unităţii, în mod deosebit la parolele acesteia.

Dacă sistemul este defect şi măsurile de precauţie enumerate nu mai pot fi luate, se recomandă ca specialiştii unităţii să fie alături de cei ce asigură întreţinerea pentru a şti cu exactitate ce anume efectuează. În acest scop, ei chiar pot fi întrebaţi de ce efectuează operaţiunile respective.

Activităţile de întreţinere trebuie să aibă un plan, în totală concordanţă cu planul de funcţionare al întregului sistem. De regulă, producătorii specifică termenele la care să se realizeze întreţinerea fiecărei componente. Numai responsabilul sistemului poate accepta efectuarea unor operaţiuni înainte de termen, precum şi repararea, înlocuirea sau înnoirea unor elemente din sistem.

Se recomandă ţinerea evidenţei materialelor de rezervă, chiar a imprimantelor, terminalelor sau monitoarelor, iar consumabilele să fie comandate la timp pentru a nu se produce disfuncţionalităţi în sistem.

Testarea securităţii sistemului trebuie să se realizeze înainte ca acesta să înceapă prelucrarea datelor reale ale unităţii.

Numele specialiştilor în întreţinere, precum şi al furnizorilor de utilităţi, trebuie să fie afişate la vedere pentru o contactare a lor în orice moment, de către persoanele autorizate să facă acest lucru.

Dacă inginerii de întreţinere solicită scoaterea din unitate a unor componente sau a documentaţiei firmei, în primul rând, trebuie să ne asigurăm că ele nu conţin date importante ale firmei. Este mult mai recomandat ca datele aflate pe unele suporturi să fie distruse, decât să se mizeze pe discreţia specialiştilor. Costă mai mult, dar e mai sigur.

„Cârpirea" softului este o altă problemă importantă. Sunt cazuri când trecerea peste un punct din program va duce la funcţionarea lui corectă în continuare, dar nimeni nu ştie exact cum funcţionează. Şi încă ceva: depinde şi de cine face „cârpeala" programului şi cu ce scop. Şi astfel de operaţiuni se scriu în registrul de întreţinere.

18.4 Toleranţa la cădere a echipamentelor

Cel mai cunoscut este sistemul din aviaţie care, în cazul când o componentă se defectează, dispune de alta care să-i preia funcţia. Unele piese, cum sunt cele de control al zborului sau a componentelor hidraulice, au câteva piese înlocuitoare, astfel încât o catastrofă majoră ar putea să apară numai după ce toate aceste piese de siguranţă s-au defectat. Toleranţa la cădere a avioanelor este asigurată astfel încât să nu aibă loc prăbuşirea lor.

În cazul calculatoarelor aceasta este o calitate foarte importantă, absolut vitală pentru existenţa sistemelor performante. Toleranţa la cădere sau la defecte trebuie să contribuie la prevenirea pierderilor sau denaturării datelor şi, pentru aceasta, orice apăsare de

tastă trebuie să fie înregistrată undeva, astfel încât să poată fi restaurată prin anumite proceduri. Toleranţa la cădere trebuie să facă în aşa fel încât să permită funcţionarea sigură, controlată şi supravegheată, în timpul reparării, asigurându-se astfel funcţionarea continuă a calculatorului care a înregistrat o defecţiune, chiar şi una majoră, în timp ce se lucrează pentru îndepărtarea ei.

În practică, aşa-ceva este destul de greu de realizat, dar, dacă numărul componentelor cu rol vital în existenţa sistemului s-ar reduce şi ar avea mai mulţi înlocuitori, operaţiunea este, totuşi, posibilă.

În sensul celor spuse până acum, sunt tipuri de calculatoare care funcţionează cu două unităţi centrale de prelucrare, în tandem, ambele prelucrând în acelaşi timp aceleaşi date şi programe. Pe această cale, la eventuala cădere a uneia dintre ele, cealaltă va funcţiona singură până când a doua va fi repusă în funcţiune. Echipamentele sunt amplasate în săli apropiate şi folosesc aceleaşi condiţii de lucru, cum ar fi: aer condiţionat, linii de comunicaţie, tipuri de unităţi de bandă şi de discuri, surse de energie electrică şi alte utilităţi. Cât timp majoritatea sistemelor cad din cauza unei plăci de memorie sau de circuite logice sau din cauza unor mici incidente înregistrate la softul de sistem sau de aplicaţii, funcţionarea în tandem evită căderea sistemului în întregime.

Alte componente ale sistemelor electronice de calcul sunt astfel construite încât să-şi exercite unele funcţii în formă dublă. Un exemplu îl oferă metoda înregistrării „în oglindă" pe disc, prin care două discuri sunt scrise în acelaşi timp pentru prevenirea pierderilor de date, dacă s-ar defecta capetele de citire-scriere ale unuia.

Echipamentele folosite în condiţii dificile, cum sunt cele mobile din domeniul militar, sunt amplasate în containere speciale, deosebit de rezistente la şocuri, apă şi praf. Sistemul de cablare va fi protejat prin ţevi metalice, iar căderile de energie vor fi suplinite de un sistem energetic propriu.

Toate măsurile luate pentru eventualele căderi trebuie să fie în deplină concordanţă şi cu importanţa întregului sistem de prelucrare automată a datelor.

18.5 Contractele

Unul dintre cele mai neplăcute momente referitoare la configuraţia sistemului îl reprezintă lungile discuţii purtate cu cei ce le-au livrat, atunci când sistemul se defectează sau nu funcţionează la parametrii aşteptaţi. Sunt cunoscute suficiente mici necazuri din lumea calculatoarelor, numai că producătorii de sisteme n-au nici un interes să le populărizeze, fie din dorinţa de a nu-şi păta reputaţia, fie mizând pe faptul că ele nu vor fi uşor sesizate.

Aproape că a devenit o regulă supraestimarea caracteristicilor calculatoarelor. Vânzătorii sunt, de cele mai multe ori, nesinceri sau prea încrezători în produsele ce le comercializează, imboldul venind de la producători, care îşi prezintă produsele ca fiind cele mai bune, în raport cu ale concurenţilor de pe piaţă.

De vină sunt şi beneficiarii care, deseori, subestimează sau nu cunosc ceea ce vor. De cele mai multe ori, vor sistemele cele mai ieftine, dar îşi schimbă părerea când le pun în funcţiune, ajungând la concluzia că era mai bine dacă acesta ar dispune şi de nişte funcţii ale căror beneficii le simte nevoia.

Totul s-ar termina cu bine dacă, din fazele incipiente ale procurării sistemului, s-ar concepe contracte care să scutească toate părţile de discuţii interminabile.

Din prima fază, clientul trebuie să ofere distribuitorului de sisteme următoarele elemente:

1. O foarte clară definire a sistemului dorit:

a) descrierea funcţiilor solicitate acestuia şi componentele cu rol prioritar din structura sa. Dacă este nevoie de un procesor de texte, atunci trebuie cerut aşa-ceva, dacă se cere un soft de birotică, trebuie menţionat ca atare; oricum, nu trebuie să ne aşteptăm ca un soft de un tip anume să ne onoreze toate pretenţiile de prelucrare automată a datelor;

b) descrierea intenţiilor de extindere a sistemului în viitor, îndeosebi dacă se vrea crearea unei reţele de calculatoare;

c) detalii privind gradul de încărcare a sistemului în perspectivă, specificându-se numărul utilizatorilor, tipul activităţilor de executat, cerinţele reţelei, importanţa ce o va avea sistemul şi, de aici, cerinţele pe linie de întreţinere şi reparare a lui.

2. Stabilirea nivelului de securitate dorit în sistem, astfel încât furnizorul să ştie ce să ofere.

3. Păstrarea tuturor documentelor referitoare la negocierile cu furnizorul de componente. Se poate merge până acolo încât să se specifice minutele de întâlniri, comentariile şi observaţiile de pe parcurs, conversaţiile telefonice, cu data corespunzătoare, cât timp au durat şi cu cine s-au purtat, ce literatură s-a consultat, ce prezentări au fost făcute de către furnizor ş.a.

4. Cuantificarea, dacă este posibilă, a efectelor defectării totale a sistemului sau a nefuncţionării lui la parametrii promişi. Furnizorii trebuie să ia cunoştinţă de aceste efecte.

5. Se vor consemna toate elementele descrise anterior într-o comandă proforma sau într-o cerere de ofertă, astfel încât furnizorul să ştie din timp ce trebuie să ofere sistemul şi să facă promisiunea onorării tuturor cerinţelor.

6. De asigurat că serviciile garantate prin contract pot fi onorate într-un timp bine determinat, stabilind cu exactitate ce misiuni revin specialiştilor, definind obligaţiile contractuale, responsabilităţile şi termenele de plată. De toate aceste aspecte trebuie să se ocupe o persoană ce va fi numită în acest sens.

Analizaţi modul în care se asigură securitatea echipamentelor într-o organizaţie cunoscută de dumneavoastră.

Anexa nr. 19

A19. Păstrarea, distrugerea şi eliminarea suporturilor informaţionale

Materialele care păstrează date supuse prelucrării automate a datelor şi cele auxiliare se păstrează în camere speciale.

Documentele ce conţin informaţii aflate sub un control special se păstrează în seifuri sau în locuri protejate prin sisteme speciale.

Operaţiunea de distrugere trebuie să urmeze proceduri speciale.

Cea mai bună cale de distrugere este *arderea*, folosită, de regulă, pentru gunoaiele informatice adunate în pungi speciale. Înaintea arderii ele trebuie păstrate în locuri cu o astfel de destinaţie. La operaţiune vor participa două persoane, care sunt obligate să ţină un registru special pentru consemnarea a ceea ce se supune arderii. Cenuşa trebuie să fie împrăştiată pentru distrugerea oricărei posibilităţi de reconstituire a datelor conţinute. La fel pot fi distruse şi alte materiale, cum sunt pachetele de discuri magnetice, după ce se recuperează anumite piese.

Transformarea în pastă este posibilă numai pentru reziduurile de hârtie, nu şi pentru banda magnetică, microfilm sau benzi tuşate.

Fărâmiţarea se aplică resturilor de hârtie, indigo, bandă magnetică, microfilm, dar o astfel de operaţiune trebuie să fie a treia şi ca utilizare. Înaintea acestei operaţiuni, în cazul benzii magnetice, în primul rând, trebuie tăiată întreaga rolă. Standardele internaţionale prevăd ca particulele rezultate din această operaţiune să nu fie mai mari de 1/32 inch. De regulă, fărâmiţarea este recomandată înaintea arderii.

O atenţie specială se va acorda suporturilor magnetice întrucât ele se pot refolosi. Dacă aceasta se întâmplă în aceeaşi unitate, noul posesor trebuie să aibă cel puţin aceeaşi autorizare pe linia accesului la informaţii ca şi precedentul. Pentru un plus de siguranţă se recomandă completarea cu zerouri a vechiului suport, sau cu cifre aleatoare. Dacă se utilizează în afara unităţii, vor fi luate măsuri suplimentare, dar oricum nu se va declara utilizarea avută anterior.

Pentru ştergerea benzilor magnetice există aparatură specială de demagnetizare, realizată de Ampex, Hewlett-Packard sau Consolidated Engineering Corp.

Discurilc magnctice sunt ştcrsc prin curcnt altcrnativ sau continuu, dacă sistemul de prelucrare automată a datelor permite o astfel de operaţiune, după care se efectuează scrierea de trei ori cu cifre 1 şi 0, şi încă o dată cu un singur caracter alfabetic.

Anexa nr. 20

A 20. Relaţii cu Terţi

Există posibilitatea ca furnizorii, prin condiţii stipulate în contracte încheiate cu ARFCN, să necesite acces la sistemul RIC. Exemple de astfel de situaţii ar putea fi: vizualizare, copiere sau modificare a datelor din jurnale cu informaţii privind accesul la RIC, instalarea, remedierea sau corectarea programelor sau sistemelor de operare, monitorizarea şi reglarea parametrilor de funcţionare ale diverselor dispozitive sau echipamente conectate la sistemul RIC. Stabilirea unor limite şi a unor controale pentru ceea ce poate fi accesat, copiat, modificat şi controlat de către furnizori va elimina sau reduce riscul aducerii de prejudicii materiale sau de natură morală ARFCN.

Scopul Regulamentului de Relaţii cu Terţi este de a stabili regulile pentru accesul furnizorilor la SI-ARFCN şi la serviciile de întreţinere (curent, apă, instalaţii de stingere a incendiilor, instalaţii de climatizare, instalaţii de control a accesului etc.) care sunt controlate prin dispozitive ce utilizează sistemul RIC, responsabilităţile ce revin furnizorului în ceea ce priveşte protecţia informaţiei în cadrul ARFCN.

1. Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale ARFCN;

În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:

- Informaţiile din cadrul ARFCN, la care Furnizorul are drept de acces;
- Modul în care informaţiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;
- Metodele de predare, distrugere sau de transfer al drepturilor informaţiilor ARFCN aflate în posesia Furnizorului, la încheierea contractului.

2. Furnizorul trebuie să folosească sistemul RIC din cadrul ARFCN numai în scopul stipulat în contract;
3. Orice altă informaţie din sistemul informatic al ARFCN obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora;
4. Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a ARFCN şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la SI al ARFCN, vor fi scoase din uz la încheierea relaţiilor contractual;
5. Accesul Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces ale ARFCN (Anexa nr. 12) şi Regulamentele de Acces (Anexa nr. 3 şi Anexa nr.4);
6. Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii ARFCN, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare;
7. În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate ARFCN sau distruse în cel mult 24 de ore de la producerea evenimentului;
8. În cazul terminării/rezilierii contractului sau la cererea ARFCN, Furnizorul va preda sau distruge toate informaţiile ce aparţin Filialei şi va oferi certificare în scris privind

predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului;

10. În cazul încheierii contractului sau la cererea ARFCN, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile ARFCN. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea ARFCN;
11. Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către ARFCN trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.

Anexa nr. 21

A 21. Licenţe de utilizare

Programele şi tehnologiile informatice sunt protejate prin Licenţe de utilizare. Acestea pot fi utilizate numai în conformitate cu prevederile Licenţelor, prevederi care trebuie cunoscute de către toţi utilizatorii SI.

Regulamentul privind Licenţele de Utilizare stabileşte reguli de utilizare a programelor informatice, precum şi a tuturor informaţiilor protejate prin Licenţe în cadrul SI-ARFCN.

1. ARFCN furnizează în limita bugetului licenţe pentru toate programele aprobate spre utilizare astfel încât angajaţii să îşi poată desfăşura munca într-un mod eficient şi rapid.
2. ARFCN trebuie să se pună de acord în mod adecvat cu furnizorii implicaţi pentru obţinerea de copii adiţionale ale licenţelor dacă şi când acestea sunt necesare în activitatea instituţiei.
3. Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele reţelei ARFCN în situaţia în care nu există aprobări specifice. **Administratorii de sistem vor şterge produsele şi toate materialele protejate prin drepturi de autor în situaţia menţionată, cu excepţia cazului în care utilizatorii implicaţi fac dovada autorizaţiei de folosire sau stocare de la producătorii de drept.**
4. Programele sau alte bunuri informatice aflate sub incidenţa drepturilor de autor aflate în posesia ARFCN nu vor fi copiate, cu excepţia cazului în care această copiere este în concordanţă cu prevederile licenţei.

Anexa nr. 22

A 22. Returnarea resurselor la terminarea contractului

Utilizatorul va returna Academiei Română Filiala Cluj-Napoca-Napoca, la încetarea contractului de muncă sau de servicii, orice informaţii şi orice mijloace de procesare a informaţiilor puse la dispoziţia sa în scopul îndeplinirii atribuţiilor de serviciu sau a obligaţiilor contractuale. Acestea includ şi nu se limitează la: credenţialele de acces la sisteme critice, primite sau modificate pe perioada contractului ş.a.m.d.

Anexa nr. 23

Lista programelor de tip shareware sau freeware utilizate în cadrul Academiei Române Filiala Clu-Napoca

Nume software	Descriere	Detalii
Adobe Acrobat Reader	Licenţă: Freeware Platformă: Windows All	**Adobe Reader** este standardul global pentru vizualizarea fisierelor PDF. Este unicul vizualizator de PDF-uri care poate deschide toate documentele PDF si interactiona cu acestea. Utilizati Adobe Reader pentru a vizualiza fisiere PDF, a cauta in acestea, a le semna digital, a le verifica, a le tipari si a le folosi in colaborari.
Adobe Flash Player	Licenţă: Freeware Platformă: Windows All	**Adobe Flash Player** iti permite sa vizualizezi continutul web interactiv ca si: jocuri, afaceri, prezentari, reclame. Pachetul include doar Flash Player. Programul Ruleaza fisiere doar prin intermediul browser-ului de web. Data de sfârşit al perioadei de asistenţă pentru Adobe Flash este pe 31 decembrie 2020.
AVG Anti-Virus Free Edition	Licenţă: Freeware Platformă: Windows All	**AVG Anti-Virus Free** Contine: Antivirus: care va protejeaza de virusi, worm, trojan. Antispyware: care va protejeaza de spyware, adware si alte programe nedorite. Anti-Rootkit: care ofera protectie impotriva rootkiturilor. Web Shield & LinkScanner: care ofera protectie impotriva accesarii siteurilor periculoase. "AVG Anti-Virus Free" este un antivirus bun si actualizat, care poate scana intreg continutul PC-ului pentru a depista virusii. Acesta poate fi de asemenea setat sa caute prin fisiere individuale sau foldere, ca si in medii externe precum CD-urile sau DVD-urile.
Endnote	Versiune Demo Platformă: Windows All	**Endnote** este un soft de gestiune bibliografica produs de Thomson Reuters ca si Reference Manager. Aceste Softuri permit constituirea de baze de date bibliografice prin introducere manuala sau prin importare de date dintr-o baza externa cum ar fi un catalog de biblioteca sau o baza de date Web.
Google Chrome	Licenţă:Freeware Platformă: Windows All	**Google Chrome** este un navigator web de tip sursa libera produs de catre Google. Numele navigatorului este derivat de la interfata grafica
Mozilla Firefox	Licenţă:Freeware Platformă: Windows All	**Mozilla Firefox** este un browser de web dezvoltat de Fundatia Mozilla
Open Office	Licenţă: Freeware Platformă: Windows	**OpenOffice.org** este un pachet de programe tip Office gratuit pentru toata lumea.

	All, Linux	
Opera	Licenţă: Freeware Platformă: Windows All	**Opera** este o suita Internet gratuita ce functioneaza pe multiple sisteme de operare. Aceasta suita contine: Browser web; Client e-mail si de stiri; Agregator de stiri; Carte de adrese; Client IRC; Gestionar de descarcari; Client BitTorrent; Opera este dezvoltat de Opera Software in Oslo, Norvegia.
Picasa	Licenţă:Freeware Platformă: Windows All, Linux	**Picasa** este un manager foto creat de Google. Picasa este un soft care permite administrarea volumelor mari de fotografii – vizualizare, organizare, editare si impartire. descarcă
Primo PDF	Licenţă: Freeware Platformă: Windows All	**PrimoPDF** este software gratuit pentru a crea fisiere PDF standard. Poate crea fisiere PDF din peste 300 de formate.
PDF24 Creator	Licenţă: Freeware Platformă: Windows All	**PDF24 Creator** este un software de aplicaţie de Geek Software GmbH pentru crearea de fişiere PDF din orice aplicaţie şi pentru convertirea fişierelor în PDF, imprimantă PDF. Aplicaţia este lansată sub licenţă freeware proprie. Software-ul a fost dezvoltat în Germania din 2006 şi este dezvoltat activ. descarcă
QuickTime	Licenţă: Freeware Platformă: Windows All	**QuickTime** este media playerul gratuit de la Apple. Cea mai noua versiune ofera suport pentu dispozitivele mobile, pentru noile formate HD-DVD si Blu-ray si poate rula sunet surround. Acesta dispune de asemenea de functii avansate precum capabilitati de streaming avansate si, peste toate acestea, are o interfata de utilizator placuta!
Total Commander	Licenţă: Demo Platformă: Windows All	**Total Commander** poate inlocui fara probleme Windows Explorer-ul. Acesta ofera suport multilingual, cautare, sincronizare de directoare, suporta arhivele ZIP, ARJ, LZH, RAR, UC2, TAR, GZ, CAB, ACE plus pluginuri, contine un client FTP inclus, suport HTTP si multe altele. Total Commander este un manager de fisiere care iti permite sa operezi usor cu fisierele si directoarele de pe hard discul tau. Suplimentar iti poate facilita conexiunea pe un FTP cat si transferul de fisiere/directoare de/pe acesta.
7-zip	Licenţă: freeware Platformă: Windows All Linux	**7-Zip** este un arhivator liber open source, creat în 1999 de Igor Pavlov. 7-Zip operează cu formatul de archivă 7z, dar poate citi şi scrie într-o serie de alte formate. Programul poate fi folosit din linie de comandă, din interfaţa grafică, sau prin meniul contextual. Formate suportate: • Packing / unpacking: 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM

		• Unpacking only: AR, ARJ, CAB, CIIM, CPIO, CramFS, DMG, EXT, FAT, GPT, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VMDK, WIM, XAR and Z. Encriptare puternica AES-256 pentru formatele 7z and ZIP
Winrar	Licenţă: Demo Platformă: Windows All	**WinRAR** este un puternic manager de arhive. El ofera un suport complet pentru tipurile de arhive RAR si ZIP, decomprima insa si tipurile 7Z, ACE, ARJ, BZ2, CAB, GZ, ISO, JAR, LZH, TAR, UUE, Z. O parte din capabilitatile WinRAR sunt: compresie puternica, creare volume, criptare, modul auto-extractor si facilitati pentru copii de siguranta.
Winzip	Licenţă: Demo Platformă: Windows All	**WinZip**. Noua versiune demo a clasicului program de compresie de fisiere WinZip, care este acum capabil sa decomprime fisierele in format RAR. Aceasta are toate caracteristicile pe care le asteptati in mod normal, ca si unele suplimentare: o compresie imbunatatita, decomprimarea fisierelor BZ2 si comprimarea fisierelor WAV fara pierderi de calitate.

Stimați utilizatori pentru căutarea alternativelor gratuite la soft-urile comerciale în Google se întroduce expresia: "freeware alternative Numele soft-ului comercial"

Anexa nr. 24

A 24. Lista aplicaţiilor software permise a fi folosite în cadrul Academiei Române Filiala Cluj-Napoca

--- lista în curs de completare---
- fiecare responsabil IT va adăuga aplicațiile care sunt utilizate la nivelul Institutului propriu-

- **Sistem de operare**:
  Windows
  Linux, Ubuntu
- **Aplicaţii software**:
  Microsoft Office, Open Office
  Adobe
  Legis
  Microsoft Visual, Crystal Reports
  FoxPro
  WinISIS, Aleph 500
  Total Commander
  BRD, OPFV,
  web.whatsapp.com
  Primo PDF, PDF24 Creator, doPDF
  QuickTime
  7-zip, Winrar, Winzip
  Revisal
  Nero, ImgBurn
  Corel, SWP
  Winedit pachet, Scientific Workplace 5.5 for windows

- **Browsere:**
  Internet Explorer
  Chrome
  Microsoft Edge
  Mozilla Firefox
  Opera
- **Aplicaţii software tip Antiviruşi:**
  BitDefender
  AVG
  Malwarebytes
  Windows Malicious Removal Tool
  Avast
  Avira
  Eset Nod32
  Alt tip freeware