Entitatea publică: **Institutul de Cercetare a Calităţii Vieţii**

Comisie: **Comisie Monitorizare**

PROCEDURĂ DOCUMENTATĂ privind

Securitatea IT

COD: **PS-SCIM-23**

Documente de referinţă:

Ordin 600/2018 pentru aprobarea Codului controlului intern/managerial al entităților publice

Ediţia: **a II-a**

Revizia: **0**

Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției

Nr. Crt	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
1	Elaborat	Zaharia Florin-Constantin	Asistent cercetare	18.05.2026	
2	Avizat	Cace Sorin	Presedinte Comisie Monitorizare	18.05.2026	
3	Aprobat	Cace Sorin	Director institut de cercetare	18.05.2026	

Cuprins

Pagina de gardă 1

Cuprins 2

Scopul procedurii 3

Domeniul de aplicare 3

Documente de referință 4

Definiții și abrevieri 5

Descrierea activității sau procesului 6

Responsabilități 9

Formular de evidenţă a modificărilor 9

Formular de analiză a procedurii 9

Formularul de distribuire/difuzare 10

Anexe 11

Precizări 11

Scopul procedurii

1 Stabilește modul de realizare a activității, compartimentele și persoanele implicate

Scopul procedurii este stabilirea unei metodologii unitare privind securitatea IT, utilizarea resurselor informatice ale instituției și protecția datelor, inclusiv a datelor cu caracter personal.

2 Dă asigurări cu privire la existența documentației adecvate derulării activității

Stabilirea responsabilităţilor privind întocmirea, avizarea şi aprobarea documentelor aferente acestei activităţi.

3 Asigură continuitatea activității, inclusiv în condiții de fluctuație ale personalului

Prin procedură se urmărește asigurarea continuității utilizării resurselor IT, protejarea informațiilor și a datelor cu caracter personal, prevenirea accesului neautorizat și reducerea riscurilor de incident de securitate informatică.

4 Sprijină auditul și/sau alte organisme abilitate în acțiuni de auditare și/sau control, iar pe manager, în luarea deciziei

- Nu este cazul

5 Alte scopuri

- Nu este cazul

Domeniul de aplicare

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

Procedura se referă la activitatea de securitate IT, utilizarea resurselor informatice ale instituției și protecția datelor, inclusiv a datelor cu caracter personal.

2 Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate de entitatea publică:

De activitatea procedurată depind toate activitățile instituției care utilizează resurse informatice, comunicații electronice, echipamente IT, aplicații, platforme online sau date stocate/prelucrate în format electronic.

3 Listarea principalelor activități de care depinde și/sau care depind de activitatea procedurată:

De activitatea procedurată depinde securitatea sistemelor informatice utilizate în cadrul Institutului de Cercetare a Calității Vieții.

4 Listarea compartimentelor furnizoare de date și/sau beneficiare de rezultate ale activității procedurate:

4.1 Compartimente furnizare de date

Toate structurile

4.2 Compartimente beneficiare de rezultate:

Toate structurile

4.3 Compartimente implicate în procesul activităţii:

Toate structurile ICCV; conducerea instituției; responsabilii compartimentelor; salariații ICCV; asistentul de cercetare cu atribuții IT sau furnizorul de servicii IT, după caz; responsabilul cu protecția datelor, după caz; Comisia de Monitorizare.

Documente de referință

1. Reglementări internaționale:

- Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE

2. Legislație primară:

- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările și completările ulterioare
- Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României.

3. Legislație secundară:

- Ordin nr. 600/2018 al Secretariatului General al Guvernului privind aprobarea Codului controlului intern managerial al entităţilor publice Publicat in Monitorul Oficial, Partea I nr. 387 din 07.05.2018

4. Alte documente, inclusiv reglementări interne ale entității publice:

- Programul de dezvoltare a SCIM
- Regulamentul de organizare și funcționare a instituției
- Regulamentul Intern al Instituției
- Decizii ale Conducătorului Instituției
- Politici, instrucțiuni, recomandări și ghiduri aplicabile în domeniul securității cibernetice, emise de autoritățile competente, după caz
- Circuitul documentelor
- Alte acte normative

Definiții și abrevieri

1. Definiții ale termenilor:

Nr. Crt.	Termenul	Definiția și / sau, dacă este cazul, actul care definește termenul
1.	Procedură documentată	Modul specific de realizare a unei activităţi sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem şi proceduri operaţionale
2.	Procedura de sistem (procedură generală)	Descrie un proces sau o activitate care se desfăşoară la nivelul entității publice aplicabil/aplicabilă majorității sau tuturor compartimentelor dintr-o entitate publică;
3.	Document	Act prin care se adevereşte, se constată sau se preconizează un fapt, se conferă un drept, se recunoaşte o obligaţie respectiv text scris sau tipărit inscripţie sau altă mărturie servind la cunoaşterea unui fapt real actual sau din trecut
4.	Aprobare	Confirmarea scrisă, semnătura şi datarea acesteia, a autorităţii desemnate de a fi de acord cu aplicarea respectivului document în unitate.
5.	Verificare	Confirmare prin examinare şi furnizare de dovezi obiective de către autoritatea desemnată (verificator), a faptului că sunt satisfăcute cerinţele specificate, inclusiv cerinţele Comisiei de Monitorizare.
6.	Gestionarea documentelor	Procesul de administrare a documentelor unei entităţi publice, pentru a servi intereselor acesteia, pe parcursul întregii lor durate de viaţă, de la început, prin procesul de creare, revizuire, organizare, stocare, utilizare, partajare, identificare, arhivare şi până la distrugerea lor;
7.	Ediție procedură	Forma actuală a procedurii; Ediția unei proceduri se modifică atunci când deja au fost realizate 3 revizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare;
8.	Revizie procedură	Acţiunea de modificare respectiv adăugare sau eliminare a unor informaţii, date, componente ale unei ediții a unei proceduri, modificări ce implică de regulă sub 50% din conținutul procedurii;.
9.	Sistem	Ansamblu de elemente corelate sau în interacţiune
10.	Entitate publică	Autoritate publică, instituţie publică, companie/societate naţională, regie autonomă, societate la care statul sau o unitate administrativ-teritorială este acţionar majoritar, cu personalitate juridică, care utilizează /administrează fonduri publice şi/sau patrimoniu public
11.	Securitate IT	Ansamblul măsurilor organizatorice și tehnice prin care sunt protejate echipamentele, sistemele informatice, conturile de utilizator, rețelele, aplicațiile și datele utilizate în activitatea instituției
12.	Resurse informatice / resurse IT	Totalitatea echipamentelor, aplicațiilor, conturilor, serviciilor electronice, rețelelor, platformelor online și datelor utilizate în activitatea instituției.
13.	Incident de securitate IT	Eveniment sau suspiciune de eveniment care poate afecta confidențialitatea, integritatea, disponibilitatea sau funcționarea normală a sistemelor informatice ori a datelor instituției.
14.	Credențiale de autentificare	Date utilizate pentru identificarea și autentificarea unui utilizator, precum numele de utilizator, parola, codurile de autentificare sau alte mijloace similare.
15.	Copie de siguranță / backup	Copie a datelor sau sistemelor informatice realizată în scopul restaurării acestora în cazul pierderii, deteriorării, ștergerii accidentale sau compromiterii datelor.

2. Abrevieri ale termenilor:

Nr. Crt.	Abrevierea	Termenul abreviat
1.	P.S.	Procedura de sistem
2.	Ed.	Ediție
3.	Rev.	Revizie
4.	SCIM	Sistem de Control Intern/Managerial
5.	HG	Hotărâre de Guvern

6.	ICCV	Institutul de Cercetare a Calității Vieții
7.	IT	Tehnologia informaţiei

Descrierea activității sau procesului

1. Generalități:

Procedura cuprinde regulile generale privind utilizarea resurselor informatice ale ICCV, protecția datelor și informațiilor gestionate în format electronic, prevenirea accesului neautorizat, utilizarea conturilor și credențialelor, realizarea copiilor de siguranță, raportarea incidentelor de securitate IT și responsabilitățile personalului implicat.

2. Documente utilizate:

2.1. Lista și proveniența documentelor:

- Documentele utilizate în elaborarea prezentei proceduri sunt cele enumerate la Documentele de referintă, precum și anexele dacă este cazul.

2.2. Conținutul și rolul documentelor:

- Documentele utilizate în elaborarea prezentei proceduri au rolul de a reglementa modalitatea de implementare a activității procedurate.

2.3. Circuitul documentelor:

- Pentru asigurarea condiţiilor necesare cunoaşterii și aplicării de către salariaţii entității a prevederilor legale care reglementează activitatea procedurată, elaboratorul va difuza procedura conform Formularului de distribuire/difuzare.

3. Resurse necesare:

3.1. Resurse materiale:

- Echipamente IT;
- Conexiune internet;
- Aplicații și servicii informatice utilizate de instituție;
- Soluții antivirus/antimalware, după caz;
- Sisteme sau mijloace de realizare a copiilor de siguranță;
- Imprimantă, copiator, consumabile, hârtie, dosare, după caz.

3.2. Resurse umane:

- Directorul ICCV;
- Directorul adjunct;
- Comisia de Monitorizare;
- Responsabilii compartimentelor;
- Salariații instituției;
- Asistentul de cercetare cu atribuții IT sau furnizorul de servicii IT, după caz;
- Responsabilul cu protecția datelor, după caz.

3.3. Resurse financiare:

- Conform Bugetului aprobat al Instituției

4. Modul de lucru:

4.1. Planificarea operațiunilor și acțiunilor activității:

Operațiunile și acțiunile privind securitatea IT se derulează la nivelul tuturor structurilor ICCV, prin aplicarea regulilor stabilite în prezenta procedură, cu respectarea atribuțiilor conducerii instituției, ale responsabililor compartimentelor, ale salariaților și ale persoanei/persoanelor cu atribuții IT sau ale furnizorului de servicii IT, după caz.

4.2. Derularea operațiunilor și acțiunilor activității:

ICCV asigură securitatea informației, a resurselor informatice și a datelor prelucrate în activitatea instituției, prin aplicarea următoarelor măsuri:

- Accesul terților la echipamentele IT, rețelele, aplicațiile sau datele instituției se realizează numai cu acordul conducerii instituției sau al persoanei desemnate, sub supraveghere, după caz. În contractele sau comenzile încheiate cu terții se includ, atunci când este cazul, clauze privind confidențialitatea, securitatea informației și protecția datelor cu caracter personal;
- Informațiile gestionate de instituție pot avea grade diferite de sensibilitate și importanță. Datele cu caracter personal, datele de cercetare, datele financiar-contabile, documentele interne și informațiile privind activitatea instituțională se protejează în funcție de natura, conținutul și riscurile asociate acestora;
- Obligațiile salariaților privind securitatea IT, confidențialitatea informațiilor și protecția datelor se stabilesc prin contractul individual de muncă, fișa postului, regulamentul intern, prezenta procedură și alte documente interne aplicabile;
- Parolele utilizate pentru autentificare sunt șiruri de caractere individuale și confidențiale, adecvate din punct de vedere al securității ca lungime și compoziție, formate din cel puțin 8 caractere și conținând, de regulă, combinații de litere mari și mici, cifre și/sau caractere speciale. Parolele nu se afișează, nu se comunică altor persoane și nu se utilizează de către alte persoane decât titularul contului.
- Sistemele IT ale instituției sunt protejate, în funcție de posibilitățile tehnice și resursele disponibile, prin măsuri de prevenire, detectare și limitare a accesului neautorizat, a programelor malițioase, a pierderii datelor și a altor incidente de securitate IT;
- Este interzisă modificarea neautorizată a echipamentelor IT, a configurațiilor, a aplicațiilor instalate sau a setărilor de securitate;
- Fișierele și suporturile externe, inclusiv atașamentele la e-mail, dispozitivele USB, hard-diskurile externe sau alte medii de stocare, se verifică prin mijloace antivirus/antimalware înainte de utilizare, acolo unde este tehnic posibil;
- Resursele IT ale ICCV se utilizează în scop profesional, pentru îndeplinirea atribuțiilor de serviciu. Este interzisă utilizarea acestora pentru activități contrare legii, regulamentelor interne, securității sistemelor informatice sau intereselor instituției;
- Infrastructura IT relevantă a instituției - servere, echipamente de rețea, website, aplicații sau alte sisteme informatice, după caz - este supusă periodic unor verificări sau scanări de vulnerabilitate, în funcție de resursele și posibilitățile tehnice existente;
- Intervențiile asupra echipamentelor IT, sistemelor informatice, conturilor, aplicațiilor sau configurațiilor de securitate se realizează numai de către persoane autorizate de conducerea ICCV sau de furnizori de servicii IT acceptaţi de ICCV;
- Utilizarea echipamentelor IT ale instituției de către persoane care nu fac parte din personalul ICCV se poate realiza numai cu acordul conducerii instituției sau al persoanei desemnate, sub supraveghere, după caz;
- Credențialele de autentificare — nume de utilizator, parolă, coduri de autentificare sau alte mijloace similare — sunt individuale și nu se transmit altor persoane. Fiecare salariat este responsabil pentru utilizarea conturilor care i-au fost alocate și pentru păstrarea confidențialității credențialelor. Este interzisă utilizarea credențialelor aparținând altui salariat;
- Fiecare salariat are obligația de a proteja informațiile și datele la care are acces în exercitarea atribuțiilor de serviciu, în special datele cu caracter personal, împotriva accesului neautorizat, divulgării, modificării, pierderii, distrugerii sau utilizării necorespunzătoare;
- Persoanele sau furnizorii care dezvoltă, administrează ori testează sisteme IT pentru instituție nu au acces la date cu caracter personal, cu excepția situațiilor în care accesul este necesar, autorizat și realizat cu respectarea legislației aplicabile. Pentru testare sau dezvoltare se utilizează, de regulă, date anonimizate sau seturi de date fără caracter personal;
- Este interzisă notarea, stocarea sau transmiterea parolelor în mod nesecurizat ori în locuri accesibile persoanelor neautorizate. Parolele administrative sau alte credențiale critice pot fi păstrate numai în condiții controlate, stabilite de conducerea instituției sau de persoana/persoanele cu atribuții IT;
- Stația de lucru se blochează ori de câte ori salariatul părăsește biroul sau nu utilizează calculatorul, pentru a preveni accesul neautorizat;

- După terminarea programului, calculatorul va fi închis, cu excepția operațiilor de mentenanță sau back-up;
- Este interzisă realizarea, salvarea, transmiterea sau tipărirea de capturi de ecran ori fotografii ale ecranului care conțin date cu caracter personal, documente interne sau informații confidențiale, cu excepția situațiilor justificate de atribuțiile de serviciu și autorizate potrivit regulilor interne ale instituției;
- Este interzisă transmiterea documentelor interne, a datelor sau a altor informații ale instituției către persoane neautorizate ori în afara cadrului atribuțiilor de serviciu;
- Se realizează copii de siguranță pentru datele și sistemele informatice relevante ale instituției, cu periodicitate stabilită în funcție de importanța datelor, riscurile asociate și posibilitățile tehnice existente. Asistentul de cercetare cu atribuții IT sau furnizorul de servicii IT, după caz, verifică periodic posibilitatea de restaurare a datelor din copiile de siguranță.

ICCV poate restricționa, gestiona sau monitoriza fluxurile de date din interiorul rețelei informatice, precum și accesul la internet, prin mijloace hardware și software, în scopul asigurării securității sistemelor informatice și a informațiilor stocate. Aceste măsuri se realizează cu respectarea principiilor de necesitate, proporționalitate și informare prealabilă a salariaților, potrivit legislației aplicabile și reglementărilor interne ale instituției.
Accesul utilizatorilor, interni sau de la distanță, la rețelele, sistemele informatice și aplicațiile instituției se realizează prin mecanisme de autentificare adecvate nivelului de risc și posibilităților tehnice existente. Conturile de utilizator trebuie să fie individuale și să permită, după caz, identificarea persoanei care accesează sistemul.
Sistemele informatice interne, serviciile de poștă electronică, website-ul instituției, platformele online și aplicațiile de tip cloud se securizează, în funcție de platformă și de posibilitățile tehnice, prin metode adecvate, precum conexiuni criptate, precum https, autentificare multifactor, actualizări de securitate, controlul drepturilor de acces și alte măsuri tehnice disponibile.
Documentele și datele relevante pentru activitatea instituției se pot stoca și în format electronic, cu respectarea regulilor privind accesul, confidențialitatea, integritatea, arhivarea și realizarea copiilor de siguranță.
Serverele, echipamentele de rețea și alte echipamente IT critice se amplasează, pe cât posibil, în spații protejate fizic, cu acces limitat la persoanele autorizate.

4.3. Valorificarea rezultatelor activității:

Rezultatele activității sunt valorificate la nivelul tuturor structurilor ICCV, prin utilizarea în condiții de securitate a resurselor IT, protejarea datelor și informațiilor instituției și reducerea riscurilor de incident de securitate IT.

Responsabilități

Directorul ICCV:
- aprobă procedura;
- asigură implementarea și menținerea procedurii;
- stabilește atribuțiile și responsabilitățile ce pot fi delegate pentru funcțiile subordonate;
- dispune, după caz, măsurile necesare pentru prevenirea, limitarea sau remedierea incidentelor de securitate IT.

Directorul adjunct ICCV:
- sprijină directorul ICCV în implementarea și menținerea prezentei proceduri;
- urmărește, în limitele atribuțiilor stabilite prin actele interne ale instituției și/sau prin delegare, aplicarea măsurilor privind securitatea IT;
- coordonează operațional, după caz, relația dintre conducerea instituției, persoana/persoanele cu atribuții IT sau furnizorul de servicii IT, Comisia de Monitorizare și celelalte structuri implicate;
- informează directorul ICCV cu privire la riscurile, incidentele sau dificultățile relevante semnalate în aplicarea procedurii;
- sprijină punerea în aplicare a măsurilor dispuse de conducătorul instituției pentru prevenirea, limitarea sau remedierea incidentelor de securitate IT.

Comisia de Monitorizare
- monitorizează implementarea prezentei proceduri în cadrul SCIM;
- analizează, după caz, necesitatea actualizării procedurii;
- include aspectele relevante privind securitatea IT în activitățile de monitorizare, evaluare și raportare specifice SCIM.

Asistentul de cercetare cu atribuții IT și alte persoane cu atribuții IT:
- administrează, după caz, conturile de utilizator, drepturile de acces, echipamentele și sistemele informatice ale instituției;
- asigură, în funcție de atribuții, resurse și posibilități tehnice, actualizările, protecția antivirus/antimalware, copiile de siguranță și măsurile tehnice de securitate;
- sprijină conducerea instituției în identificarea, limitarea și remedierea incidentelor de securitate IT;
- informează conducerea instituției cu privire la riscurile tehnice relevante identificate.

Responsabilii de compartimente:
- sesizează directorului ICCV, directorului adjunct și persoanei/persoanelor cu atribuții IT orice incident, risc sau suspiciune de incident de securitate IT despre care iau cunoștință;
- sprijină, la nivelul structurii/compartimentului coordonat, aplicarea măsurilor dispuse pentru prevenirea, limitarea sau remedierea incidentelor de securitate IT;
- transmit salariaților din structura/compartimentul coordonat comunicările și instrucțiunile primite de la conducerea instituției privind securitatea IT.

Salariații ICCV:
- utilizează resursele IT ale instituției numai în scop profesional și cu respectarea prezentei proceduri;
- păstrează confidențialitatea credențialelor de autentificare;
- protejează informațiile și datele la care au acces în exercitarea atribuțiilor de serviciu;
- nu instalează aplicații, nu modifică setări și nu intervin asupra echipamentelor IT fără autorizare;
- blochează stația de lucru atunci când părăsesc biroul;
- raportează de îndată persoanei/persoanelor cu atribuții IT orice incident sau suspiciune de incident de securitate IT.

Responsabilul cu protecția datelor personale:
- acordă puncte de vedere, după caz, cu privire la aspectele care implică protecția datelor cu caracter personal;
- sprijină analizarea obligațiilor de notificare sau documentare în cazul incidentelor care pot afecta date cu caracter personal.

Formular de evidenţă a modificărilor

Nr. Crt	Numărul ediţiei / reviziei	Data ediţiei / reviziei	Componenta revizuită	Descrierea modificării	Avizul conducătorului compartimentului
1	Ediția I	07.05.2018	X	X	
2	Ediția a II-a	18.05.2026	Scopul procedurii; domeniul de aplicare; documente de referință; definiții și abrevieri; descrierea activității sau procesului; responsabilități.	Actualizarea procedurii privind securitatea IT prin completarea cadrului de referință, clarificarea regulilor de utilizare a resurselor IT, a măsurilor de protecție a datelor, a regulilor privind autentificarea, backup-ul, monitorizarea fluxurilor de date, raportarea incidentelor și responsabilitățile persoanelor implicate.	Favorabil

Formular de analiză a procedurii

Nr. Crt	Compartiment	Nume și prenume	Aviz	Data	Observaţii	Semnătura
1	Director	Cace Sorin	Favorabil	18.05.2026		

Formularul de distribuire/difuzare

Nr. Crt	Scopul difuzării	Compartiment	Nume și prenume	Data primirii	Data retragerii	Data intrării în vigoare	Semnătura
1	Aplicare, Informare	Director	Cace Sorin	18.05.2026		18.05.2026	
2	Aplicare, Informare	Director	Stănescu Iulian	18.05.2026		18.05.2026	
3	Aplicare, Informare	Biroul financiar-contabil	Dumitrescu Nicoleta	18.05.2026		18.05.2026	
4	Evidență, Arhivare, Monitorizare	Comisie Monitorizare	Stănescu Simona	20.05.2026		18.05.2026	
5	Aplicare	Politici sociale	Zaharia Florin-Constantin	18.05.2026		18.05.2026	
6	Aplicare	Politici sociale	Glăvan Eugen	18.05.2026		18.05.2026	
7	Aplicare	Calitatea vieţii	Aldea Iulian	19.05.2026		18.05.2026	

Anexe

Nr. Crt	Denumirea anexei	Elaborator	Aproba	Numar de exemplare	Arhivare

Precizări

Toate documentele și dovezile pe baza cărora se realizează activitatea procedurată se păstrează în dosarele Comisiei de Monitorizare.

Diagrama de proces

Securitatea IT

Elaborare PS

- Elaborarea PS de către persoanele desemnate
- Verificarea PS de către șeful microstructurii

Actualizarea PS în cadrul ședințelor comisiei

- Verificare conformității PS

CONFORM: **DA**

Implică mai multe structuri / microstructuri: **DA**

Avizare PS

- Structura / microstructura responsabilă transmite electronic PS structurilor / microstructurilor implicate

Observații: **NU**

Adoptare PS

Difuzare PS

- Originalul PS se înregistrează și se păstrează la structura / microstructura emitentă
- Se tranmite PS în format electronic structurilor / microstructurilor implicate și responsabilului pe linia controlului intern/managerial