Nr. înreg. 820 / 18.11.2022

PROCEDURĂ OPERAŢIONALĂ

SECURIZAREA INFORMAȚIILOR ȘI DATELOR

P.O. SCR 08

Ediţia: I-a, 18.11.2022, Revizia 1

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

Nr. Crt	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
1	2	3	4	5	6
1.1	Elaborat	Andrei Gheorghe	Secretar Șef	14.11.2022	
1.2	Elaborat	Sandu Carmen	Secretar	14.11.2022	
1.3	Verificat	Tomescu Raluca-Veronica	Presedinte comisie SCIM	16.11.2022	
1.4	Aprobat	Mareș Silvia	Director	18.11.2022	

2. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii

Nr. Crt	Ediția sau, după caz, revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
1	2	3	4	5
2.1	Ediția I-a			25.02.2022
2.2	Revizia 0			
2.3	Revizia 1			18.11.2022

3. Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii

Nr. Crt	Scopul difuzării	Ex. nr.	Compartiment	Funcția	Nume și prenume	Data primirii	Semnătura
1	2	3	4	5	6	7	8
3.1	Informare / Aplicare		Secretariat	Secretar Șef	Andrei Gheorghe	18.11.2022	
3.2	Informare / Aplicare		Secretariat	Secretar	Sandu Carmen	18.11.2022	
3.3	Aprobare		Director	Director	Mareș Silvia	18.11.2022	
3.4	Verificare		SCIM	Presedinte comisie SCIM	Tomescu Raluca-Veronica	18.11.2022	
3.5	Arhivare		Secretariat	Secretar Șef	Andrei Gheorghe		

4. Scopul procedurii

4.1. Stabilește modul de realizare a activității, compartimentele și persoanele implicate

Scopul acestei proceduri este de a stabili normele de practică privind asigurarea securității informației electronice și a datelor. Securizarea se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul unității, sunt proprietatea scolii în condițiile legilor în vigoare.

4.2. Dă asigurări cu privire la existența documentației adecvate derulării activității

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

4.4. Sprijină auditul și/sau alte organisme abilitate în acțiuni de auditare și/sau control, iar pe director, în luarea deciziei

4.5. Alte scopuri

5. Domeniul de aplicare

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

- Se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a unității. Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile procedurii:
- Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- Colaboratorii care au acces la sistem;
- Furnizorii care au acces la sistem;
- Elevii;
- Alte persoane, entități sau organizații care au acces la sistem.

5.2. Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate de unitate:

- Operaţiunea se desfăşoară în cadrul activităţii de management din cadrul Unității.

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

a. Această activitate depinde de activitatea compartimentelor:
- Personal didactic;
- Conducere;
- Comisia de Evaluare și Asigurare a Calității;
- Secretariat.

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

5.4.1. Compartimente furnizoare de date:

- Toate compartimentele.

5.4.2. Compartimente furnizoare de rezultate:

- Toate compartimentele.

5.4.3. Compartimente implicate în procesul activităţii:

- Toate compartimentele.

6. Documente de referință

6.1. Reglementări internaționale:
- Nu este cazul.

6.2. Legislație primară:
- Legea Educației Nr. 1/2011 – cu modificările și actualizările ulterioare;
- Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare;
- Legea nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea ANSPDCP, precum și pentru abrogarea Legii nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea ANSPDCP, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare;
- Legea nr. 455/2001 privind semnătura electronică, cu modificările și completările ulterioare.

6.3. Legislație secundară:
- Ordin nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităţilor publice Publicat in Monitorul Oficial, Partea I nr. 387 din 07.05.2018;
- Instrucţiunea nr. 1/2018 din 16 mai 2018 privind aplicarea unitară la nivelul unităţilor de învăţământ preuniversitar a Standardului 9 - Proceduri prevăzut în Codul controlului intern managerial al entităţilor publice, aprobat prin Ordinul secretarului general al Guvernului nr. 600/2018.

6.4. Alte documente, inclusiv reglementări interne ale unității:
- Regulamentul de organizare şi funcţionare al unității;
- Regulamentul Intern al unității;
- Decizii ale Conducătorului unității;
- Circuitul documentelor;
- Alte acte normative;

7. Definiții și abrevieri

7.1. Definiții ale termenilor:

Nr. Crt	Termenul	Definiția și / sau, dacă este cazul, actul care definește termenul
1	2	3
7.1.1	Procedură documentată	Modul specific de realizare a unei activități sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem şi proceduri operaţionale;
7.1.2	Procedură 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;
7.1.3	Procedură operaţională (procedură de lucru)	Procedură care descrie un proces sau o activitate care se desfăşoară la nivelul unuia sau mai multor compartimente dintr-o entitate, fără aplicabilitate la nivelul întregii entități publice;
7.1.4	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;
7.1.5	Aprobare	Confirmarea scrisă, semnătura şi datarea acesteia, a autorităţii desemnate de a fi de acord cu aplicarea respectivului document în organizaţie;
7.1.6	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;
7.1.7	Ediţie a unei proceduri operaţionale	Forma iniţială sau actualizată, după caz, a unei proceduri operaţionale, aprobată şi difuzată;
7.1.8	Revizia în cadrul unei ediţii	Acţiunile de modificare, adăugare, suprimare sau alte asemenea, după caz, a uneia sau mai multor componente ale unei ediţii a procedurii operaţionale, acţiuni care au fost aprobate şi difuzate.

7.2. Abrevieri ale termenilor:

Nr. Crt	Abrevierea	Termenul abreviat
1	2	3
7.2.1	P.S.	Procedură de sistem
7.2.2	P.O.	Procedură operațională
7.2.3	E	Elaborare
7.2.4	V	Verificare
7.2.5	Ap.	Aplicare
7.2.6	Ah.	Arhivare

8. Descrierea procedurii

8.1. Generalități:

Securizarea datelor se face atât din punct de vedere fizic cât și logic.
Securitatea fizică a unui sistem informatic constă in asigurarea securității componentelor hardware a unui sistem informatic și anume protejarea împotriva furtului sau vandalizării acestora prin plasarea lor într-o încăpere sigură.
De asemenea, trebuie asigurată paza și accesul persoanelor străine.
O alta securitate fizică care trebuie avută în vedere este securitatea care are ca obiect copiile datelor si programelor salvate (backup). Aceste copii trebuie protejate împotriva furtului, vandalizării lor.
Pe lângă securitatea fizică este necesară și asigurarea securității logice.
Pentru a avea efectul scontat acestea trebuie să existe concomitent. Având în vedere că un sistem informatic conține pe lângă date și o serie de servicii și mai multe tipuri de acces din punct de vedere al securității logice.

8.2. Documente utilizate:

8.2.1. Lista și proveniența documentelor:

- Documentele utilizate în elaborarea prezentei proceduri sunt cele enumerate la pct.6.

8.2.2. Conținutul și rolul documentelor:

- Documentele utilizate în elaborarea prezentei proceduri au rolul de a reglementa modalitatea de implementare a activității procedurate;
- Accesul, pentru fiecare Compartiment, la legislaţia aplicabilă, se face prin programul informatic la care au acces salariaţii unității.

8.2.3. Circuitul documentelor:

- Pentru asigurarea condiţiilor necesare cunoaşterii și aplicării de către salariaţii unității a prevederilor legale care reglementează activitatea procedurată, elaboratorul va difuza procedura conform pct.3.

8.3. Resurse necesare:

8.3.1. Resurse materiale:

- Computer;
- Imprimantă;
- Copiator;
- Consumabile (cerneală/toner);
- Hârtie xerox;
- Dosare.

8.3.2. Resurse umane:

- Conducătorul unității;
- Compartimentele prevăzute în organigrama unității.

8.3.3. Resurse financiare:

- Conform Bugetului aprobat al unității.

8.4. Modul de lucru:

8.4.1. Planificarea operațiunilor și acțiunilor activității:

Operațiunile și acțiunile privind activitatea procedurată se vor derula de către toate compartimentele implicate, conform instrucțiunilor din prezenta procedură.

8.4.2. Derularea operațiunilor și acțiunilor activității:

Securizarea informațiilor electronice în cadrul unității se implementează pe două nivele:

- nivelul fizic;
- nivelul logic.

Nivelul fizic de securizare a informațiilor digitale implică:

1. amplasarea serverelor de date si a echipamentelor de comunicație critice în locații izolate, dotate cu minim 2 încuietori si sisteme de alarmă pentru incendiu;
2. toate echipamentele de stocare a datelor sunt prevăzute cu surse neîntreruptibile de alimentare, cu autonomie de minim 2 ore;
3. accesul fizic la serverele de date si echipamentele de comunicație critice se face numai de către personalul autorizat;
4. fiecare intervenție fizică la serverele de date este înregistrată într-un jurnal care conține data si ora accesului, operațiile efectuate, data și ora plecării;
5. stațiile de lucru ale personalului sunt amplasate în încăperi dotate minim cu încuietoare, si dispuse astfel încât să nu permită vizualizarea facilă a ecranului de către alte persoane.

Nivelul logic de securizare a informațiilor digitale implică:

1. fiecare stație de lucru și / sau server de date / echipament de stocare date / echipament de comunicație sunt protejate prin parolă;
2. în cazul stațiilor de lucru ale personalului, gestiunea parolelor de acces la computer cade în sarcina utilizatorului, acesta fiind singurul care răspunde pentru integritatea și securitatea informațiilor stocate pe calculatorul său;
3. în cazul serverelor și a echipamentelor de comunicație, gestiunea parolelor de acces cade în sarcina responsabilului;
4. parolele de acces sunt informații care nu se divulgă terților (inclusiv rudelor de gradul I);
5. bazele de date sunt protejate prin parole de acces și prin efectuarea de copii de siguranță la intervale cuprinse între 24 de ore și 7 zile;
6. sistemele de operare tip server, precum și echipamentele de comunicație critice (routere, switch-uri) sunt protejate prin parole de acces având lungimea minimă de 10 caractere, schimbate periodic la interval de 14 zile;
7. serverele de date sunt protejate prin firewall și sunt monitorizate permanent pentru sesizarea oricăror disfuncționalități. Monitorizarea se face atât manual, prin consultarea zilnică a jurnalelor (loguri), cât și automatizat, prin emiterea de e-mailuri și/sau SMS-uri atunci când un serviciu de date își întrerupe activitatea;
8. toate căile de acces Internet (gateways) sunt prevăzute cu firewall incluziv;
9. Sistemul informatic financiar-contabil și sistemul informatic privind resursele umane, cât și celelalte sisteme informatice folosite de către personal sunt protejate cu parola de acces având lungimea minimă de 10 caractere, și se schimbă periodic la interval de 14 zile.

Arhivarea / salvarea bazelor de date poate fi:

Arhivarea unei baze de date a unui sistem informatic - rezultă o arhivă a acelui program informatic. Numele arhivei trebuie să fie unic, să nu se suprapună o arhivă cu alta.
Arhivarea întregii baze de date a programelor informatice - se recomandă măcar o dată pe lună. Arhivele nu se vor suprapune, fiecare are un nume distinct.
Arhivarea tuturor bazelor de date. Se face când se dorește mutarea bazelor de date pe alt calculator.
Atenție, arhivarea completă trebuie făcută obligatoriu înainte de reinstalări ale sistemului de operare (windows) sau când se dorește copierea pe alt calculator. Pentru salvarea totală a bazei sistemului informatic se recomandă apelarea la serviciile furnizorului aplicației informatice deoarece pot fi configurări speciale ce trebuie făcute, caz în care se pot pierde datele dacă nu se procedează corect.

Configurații de securitate a componentelor hardware pentru echipamente mobile, stații de lucru și servere.
Asupra rețelelor Internet cât și a celor interne deja compromise de atacatori, programe automate de atac informatic caută în mod constant rețele țintă pentru a găsi sisteme care au fost configurate cu software vulnerabil instalat. Configurațiile implicite sunt adesea orientate pentru a ușura exploatarea, utilizarea sistemelor, nefiind însă securizate și lăsând servicii inutile exploatabile în starea implicită a acestora.

Tehnicile de atac, încearcă să exploateze în acest fel atât serviciile accesibile via rețea, cât și software-ul de navigare al clientului.

Măsurile de protecție împotriva acestor tehnici de atac includ achiziția de componente pentru sisteme și rețea cu configurații de securitate deja implementate, instalarea sistemelor preconfigurate pentru securitate, actualizarea configurațiilor periodic și urmărirea acestora în cadrul unui sistem de management al configurațiilor.

Aceste măsuri se pot implementa prin crearea de imagini ale sistemelor și stocarea pe servere securizate împreună cu utilizarea instrumentelor de management al configurațiilor.

În funcție de soluția adoptată, aceste instrumente pot monitoriza în mod activ devierile de la configurațiile implementate, furnizând informațiile necesare pentru asigurarea utilizării configurațiilor stabilite și vor include următoarele funcționalități:
- Identificarea oricăror modificări / schimbări în cadrul unei imagini securizate care pot include modificări aduse pentru fișiere cheie, porturi, fișiere de configurații sau pentru software-ul instalat;
- Compararea imaginii fiecărui sistem cu imaginea oficială stocată în mod securizat în cadrul sistemului de management al configurațiilor;
- Blocarea instalării și prevenirea executării odată cu alertarea personalului administrativ.

Configurații de securitate pentru echipamente de rețea – Firewall, Router, Switch
Atacatorii profită de o practică des întâlnită în configurarea nivelului de securitate pe anumite echipamente de rețea: utilizatorii solicită excepții temporare din considerente specifice, de business, aceste excepții sunt aplicate dar nu și îndepărtate imediat ce necesitatea de business dispare. În unele situații și mai grave, riscul de securitate al unei astfel de excepții nu este nici analizat corespunzător nici evaluat din punct de vedere al necesității. Atacatorii caută brețele din firewall-uri, routere și switch-uri și apoi le folosesc în scopul penetrării sistemului. Atacatorii au exploatat deficiențele acestor echipamente de rețea pentru a obține accesul în mediile vizate, pentru a redirecta traficul înspre o altă rețea sau un sistem malițios ce se anunță că un sistem de încredere, și pentru a intercepta și altera informații pe măsură ce acestea sunt transmise. Cu astfel de acțiuni atacatorul obține acces la date sensibile, alterează informații importante sau chiar utilizează un sistem compromis pentru a „poza" într-un alt sistem de încredere din rețea.
Anumite organizații utilizează unelte comerciale de evaluare a setului de reguli de pe echipamentele de filtrare din rețea, cu scopul de a determina măsura în care acestea sunt consistente sau conflictuale. Se face astfel o verificare automată a stării filtrelor de rețea și se caută erori în seturile de reguli sau în listele de control al accesului (Access Control List – ACL) care ar putea permite servicii nedorite pe acele echipamente. Astfel de unelte ar trebui utilizate la fiecare modificare semnificativă a setului de reguli de pe firewall-uri, a ACL-urilor de pe router sau pe alte tehnologii de filtrare.

Funcționalitățile minim recomandate pentru menținerea unui control optim la nivel de echipamente de rețea:
- Identificarea oricărei modificări la nivel de echipamente de rețea, inclusiv routere, switch-uri, firewall-uri și sisteme IDS și IPS (orice schimbare în fișierele cheie, servicii, porturi, fișiere de configurație sau orice alt software instalat pe echipamente;
- Configurația fiecărui sistem trebuie comparată cu baza de date master cu imagini pentru a verifica orice modificare în configurație din punct de vedere al impactului asupra securității.

Securitatea aplicațiilor
Printre prioritățile recente ale grupurilor criminale se numără atacurile asupra vulnerabilităților aplicațiilor web-based precum și asupra aplicațiilor în general. Aplicațiile care nu fac verificări asupra volumului intrărilor generate de utilizator, nu reușesc să „sanitizeze" intrările prin filtrarea secvențelor de caractere care nu sunt necesare sau potențial malițioase sau nu inițiază „curățarea" variabilelor în mod corespunzător, fiind astfel vulnerabile la compromiterea de la distanță.

Atacurile pot fi efectuate prin „injectarea" de exploatări specifice incluzând buffer overflows, atacuri de tip SQL injection, cross-site scripting, cross-site request forgery, și click jacking de cod pentru obținerea controlului asupra sistemelor vulnerabile.

Pentru prevenirea unor asemenea atacuri, aplicațiile dezvoltate intern cât și aplicațiile third-party trebuie testate riguros pentru a identifica deficiențele de securitate. Pentru aplicațiile third-party, organizațiile trebuie să se asigure că furnizorii au efectuat testări riguroase de securitate pentru produse, iar pentru aplicațiile dezvoltate intern, organizațiile trebuie să efectueze testările de securitate sau să angajeze servicii de specialitate pentru efectuarea de astfel de testări.
Tool-urile ce testează cod sursă sau acelea pentru scanarea securității aplicațiilor web s-au dovedit a fi utile în vederea securizării, alături de verificările de securitate tip penetration testing efectuate manual de specialiști cu vaste cunoștințe de programare și expertiză în testarea de aplicații.

Funcționalități recomandate în sistemul de securitate al aplicațiilor:
- Detectarea și blocarea încercărilor de atac la nivel de aplicație;
- Testarea periodică, săptămânal sau chiar zilnic;
- Mitigarea tuturor vulnerabilităților cu risc mare din aplicațiile web accesibile din Internet – identificate cu scannere de vulnerabilități, instrumente de analiză statice și instrumente de revizuire a configurațiilor automate din bazele de date – fie prin modificarea fluxului, fie prin implementarea unui control compensatoriu.

Securitatea fizică
Documentele realizate în cadrul unității (documente școlare, acte de studii, registre, etc) se păstrează în fișete / dulapuri securizate, ale cărui chei se găsesc la secretarul și directorul unității.
Securitatea fizică reprezintă ansamblul reglementărilor, normelor şi măsurilor care au drept scop prevenirea accesului neautorizat la informaţii, precum şi a oricăror situaţii, împrejurări sau fapte de natură să pericliteze ori să compromită securitatea şi integritatea acestora.
Pentru eficientizarea sistemelor de pază şi apărare trebuie asigurată detectarea pătrunderii neautorizate prin folosirea unor modalităţi adecvate (sisteme de alarmă sau pentru inspectare vizuală). Se vă constitui în mod obligatoriu o forţă de intervenţie (sau va fi externalizat la o firmă de intervenție/paza) pentru situaţii de urgenţă.

8.4.3. Valorificarea rezultatelor activității:
Rezultatele activității vor fi valorificate de toate compartimentele din unitate.

9. Responsabilități

9.1. Conducătorul unității
- Aprobă procedura;
- Asigură implementarea și menținerea procedurii.

9.2. Secretariat
- Aplică și menține procedura;
- Realizează activitățile descrise la termenele stabilite în prezenta procedură.

10. Formular de evidenţă a modificărilor

Nr. Crt	Ediţia	Data ediţiei	Revizia	Data reviziei	Nr. pag.	Descrierea modificării	Semnătura conducătorului departamentului
1	2	3	4	5	6	7	8
10.1		25.02.2022				-	
10.2	I-a		1	18.11.2022		-	

11. Formular de analiză a procedurii

Nr. crt.	Compartiment	Conducător compartiment Nume și prenume	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil	Semnătura	Data
				Semnătura	Data	Observații		
1.	Secretariat	Andrei Gheorghe			18.11.2022			
2.	SCIM	Tomescu Raluca-Veronica			18.11.2022			
3.	Director	Mareș Silvia			18.11.2022			

12. Lista de difuzare a procedurii

Nr. ex.	Compartiment	Nume și prenume	Data primirii	Semnătura	Data retragerii	Data intrării în vigoare a procedurii	Semnătura
1	Conform Procesului Verbal de predare-primire.						

13. Anexe

Nr. Crt	Denumirea anexei	Elaborator	Aproba	Numar de exemplare	Arhivare
1	2	3	4	5	6
13.1		-	-	1	-

Cuprins