Departamentul (Direcţia): Comisie Monitorizare

PROCEDURĂ DE SISTEM

Securitatea IT

COD: PS-SCIM-26

Ediţia a III-a Revizia I

1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii DE SISTEM

Nr. Crt.	Elemente privind responsabilii/operaţiunea	Numele şi prenumele	Funcţia	Data	Semnătura
0	1	2	3	4	5
1.1	Elaborat	Lădariu Diana	Director adjunct	17.10.2022	
1.2	Verificat	Szabo Iosif	Administrator	17.10.2022	
1.3	Avizat	Orban Laura	Director adjunct	17.10.2022	
1.4	Aprobat	Pellegrini Lilla	Director	17.10.2022	

Cuprins

1. Scopul procedurii de sistem

1.1 Stabileşte modul de realizare a activităţii, compartimentele şi persoanele implicate:

Scopul procedurii este stabilirea unei metodologii unitare privind securitatea IT şi protecţia datelor.

De asemenea, prin prezenta procedură se urmăreşte stabilirea unui mod unitar de lucru pentru îndeplinirea sarcinilor aferente fişei postului pentru toţi angajaţii instituţiei implicaţi direct sau indirect în activitatea procedurată.

Nu în ultimul rând, prezenta procedură are ca scop scurtarea perioadei de acomodare la noul loc de muncă pentru noii angajaţi, furnizând informaţii concrete şi detaliate cu privire la modul de îndeplinire a sarcinilor aferente fişei postului pentru noul ocupant al acestuia.

1.2 Dă asigurări cu privire la existenţa documentaţiei adecvate derulării activităţii:

1.3 Asigură continuitatea activităţii, inclusiv în condiţii de fluctuaţie a personalului:

1.4 Sprijină auditul şi/sau alte organisme abilitate în acţiuni de auditare şi/sau control, iar pe manager, în luarea deciziei:

1.5 Alte scopuri specifice procedurii de sistem:

2. Domeniul de aplicare a procedurii de sistem

2.1 Precizarea (definirea) activităţii la care se referă procedura de sistem:

Procedura se referă la activitatea de securitate IT şi protecţia datelor.

2.2 Delimitarea explicită a activităţii procedurate în cadrul portofoliului de activităţi desfăşurate de entitatea publică:

Activitatea este relevantă ca importanţă, fiind procedurată distinct în cadrul instituţiei.

2.3 Listarea principalelor activităţi de care depinde şi/sau care depind de activitatea procedurată:

De activitatea procedurată depind toate celelalte activităţi din cadrul instituţiei, datorită rolului pe care această activitate îl are în cadrul derulării corecte şi la timp a tuturor proceselor.

2.4 Listarea compartimentelor furnizoare de date şi/sau beneficiare de rezultate ale activităţii procedurate:

2.4.1 Compartimente furnizare de date:

Toate structurile

2.4.2 Compartimente furnizoare de rezultate: Toate structurile

2.4.3 Compartimente implicate în procesul activităţii:

Comisia SCIM

3. Documente de referinţă (reglementări) aplicabile activităţii procedurate

3.1. Reglementări internaţionale:

- Nu este cazul

3.2. Legislaţie primară:

Ordinul nr. 530/2016 privind modificarea si completarea Ordinului secretarului general al Guvernului nr. 400/2015 pentru aprobarea Codului controlului intern managerial al entitatilor publice

Ordinul nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităților publice

3.3. Legislaţie secundară:

- Nu este cazul

3.4. Alte documente, inclusiv reglementări interne ale entităţii publice:

- Regulamentul de organizare şi funcţionare al instituției
- Regulamentul Intern al Instituției
- Decizii/Dispoziţii ale Conducătorului Instituției
- Circuitul documentelor
- Alte acte normative

4. Definiţii şi abrevieri ale termenilor utilizaţi în procedura operaţională

4.1. Definiţii ale termenilor:

Nr. Crt.	Termenul	Definiţia şi / sau, dacă este cazul, actul care defineşte termenul
1.	Procedura	Prezentarea formalizata, în scris, a tuturor paşilor ce trebuie urmaţi, a metodelor de lucru stabilite şi a regulilor de aplicat în vederea realizarii activităţii, cu privire la aspectul procesual. Procedura trebuie înteleasa ca un set de instructiuni scrise care fundamenteaza o actiune sau activitate repetitiva din institutia publica.
2.	Procedura de sistem	Procedura care descrie o activitate sau un proces care se desfasoara la nivelul tuturor directiilor/servicilor/compartimentelor din cadrul instituţiei, numite si "proceduri generale". Nu se considera de sistem acele proceduri care presupun doar o implicare limitata a directiilor de specialitate.
3.	Procedura operaţională	Prezentarea formalizata, în scris, a tuturor pasilor ce trebuie urmati, a metodelor de lucru stabilite si a regulilor de aplicat în vederea realizarii activitatii, cu privire la aspectul procesual. Mai sunt cunoscute si sub denumirile de „proceduri specifice", „proceduri de proces", „proceduri formalizate" etc. Metodele de lucru si procedurile formalizate sunt specifice fiecarei institutii si constituie obiectul sistemului de control managerial intern, respectiv al standardului intitulat „Proceduri". Pentru ca procedurile sa reprezinte instrumente eficiente, trebuie sa îndeplineasca un numar de conditii esentiale: Sa fie: - scrise si formalizate pentru fiecare activitate principala în parte, - simple si specifice, - actualizate în mod permanent, - aduse la cunostinta salariatilor, precum si tertilor daca este cazul

4.	Document	Dispozitii, prevederi etc. scrise pe suport de hârtie sau magnetic (diskete, CD-uri etc.), care reglementeaza modul de efectuare a unor activitati si/ sau precizeaza cerinte pentru acestea. Documentele pot fi de provenienta interna: ROF, fisele posturilor, Regulamente interne privind desfasurarea activitatii dar si externa: standarde, legi, prescriptii, instructiuni si orice alte documente cu caracter normativ, tehnice sau legislatie
5.	Aprobare	Confirmarea scrisa, semnatura si datarea acesteia, a autoritatii desemnate de a fi de acord cu aplicarea respectivului document în organizatie.
6.	Verificare	Confirmare prin examinare si furnizare de dovezi obiective de catre autoritatea desemnata (verificator), a faptului ca sunt satisfacute cerintele specificate, inclusiv cerintele SCIM.
7.	Gestionarea/ controlul documentelor	Multiplicarea, difuzarea, pastrarea, retragerea din uz si arhivarea documentelor.
8.	Ediție a unei proceduri	Forma inițiala sau actualizata, dupa caz, a unei proceduri, aprobata și difuzata
9.	Revizia în cadrul unei ediții	Acțiunile de modificare, adaugare, suprimare sau altele asemenea, dupa caz, a uneia sau a mai multor componente ale unei ediții a procedurii, acțiuni care au fost aprobate și difuzate
10.	Sistem	Ansamblu de elemente corelate sau în interactiune

4.2. Abrevieri ale termenilor:

Nr. Crt.	Abrevierea	Termenul abreviat
1.	P.S.	Procedura de sistem
2.	P.O.	Procedura operațională
3.	Ed.	Ediție
4.	Rev.	Revizie
5.	PC	Presedintele Comisiei de control managerial
6.	SCIM	Sistem de Control Intern/Managerial
7.	HG	Hotărâre de Guvern
9.	E	Elaborare
10.	V	Verificare
11.	A	Aprobare
12.	Ap.	Aplicare
13.	Ah.	Arhivare
14.	C	Centralizare

5. Descrierea procedurii

5.1. Generalităţi:

Procedura cuprinde etapele ce trebuie urmate, metodele de lucru stabilite şi regulile de aplicat în vederea cunoaşterii şi aplicării de către salariaţii entităţii a prevederilor legale care reglementează activitatea procedurată.

5.2. Documente utilizate:

5.2.1. Lista şi provenienţa documentelor:

- Documentele utilizate în elaborarea prezentei proceduri sunt cele enumerate la pct.3

5.2.2. Conţinutul şi rolul documentelor:

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

5.2.3. Circuitul documentelor:

- Pentru asigurarea condiţiilor necesare cunoaşterii şi aplicării de către salariaţii entităţii a prevederilor legale care reglementează activitatea procedurată, elaboratorul va difuza procedura conform pct.9.

5.3. Resurse necesare:

5.3.1. Resurse materiale:

- Computer
- Imprimantă
- Copiator
- Consumabile (cerneală/toner)
- Hartie xerox
- Dosare

- Conexiune internet
- Mijloace de transport

5.3.2. Resurse umane:

- Conducătorul Instituției
- Conducătorii de compartimente

5.3.3. Resurse financiare:

- Conform Bugetului aprobat al Instituției

5.4. Modul de lucru:

5.4.1. Planificarea operaţiunilor şi acţiunilor activităţii:

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

5.4.2. Derularea operaţiunilor şi acţiunilor activităţii:

Prezentare reţea calculatoare

- Entitatea publica este organizata pe compartimente. Fiecare compartiment este dotat cu echipamente de calcul.
- Atat structurile organizatorice cat si responsabilii IT pot avea acces la date.

Scop

- Scopul acestei proceduri este de a proteja sistemul împotriva utilizării interne neautorizate cat si protecţia datelor legate de operatiunile si evidentele prelucrate electronic atat de unii factori interni cat si externi care pot duce la pierderea accidentală în cazul defectării accidentale a echipamentelor pe care acestea sunt stocate.
- Problemele provenind din exterior sunt impredictibile si pot fi generate, în principal, prin accesarea de către utilizator a unor situri, internet cu risc (situri warez) deoarece la accesare acestea cer utilizatorului sa permită copierea pe calculatorul local, anulând restricţiile impuse de programul de firewall, a unor cookie care permit accesul din exterior la date situate pe calculatorul local. Programul firewall, impricit dezactivează copierea locala a componentelor cookie, dar există situri sigure care necesită totuşi folosirea acestor componente.
- De asemenea pe fiecare calculator în parte trebuie instalat antivirus şi firewall. Asigurarea resurselor informatice, aplicaţiilor şi datelor este o parte

integrantă a protecţiei activităţii si datelor unitatii.

- Realizarea unui sistem de securizare constă în implementarea unui set de proceduri, practici şi tehnologii pentru protecţia infrastructurii tehnologiilor de informaţie (IT) aplicaţiilor şi datelor asociate în cadrul unitatii.
- De asemenea procedura prevede şi măsuri de recuperare în caz de dezastre. Am putea clasifica aceste dezastre în două mari categorii:

1. Dezastre care afectează integritatea datelor şi nu afectează partea hardware a computerelor, cum ar fi viruşi, atacuri maliţioase, ştergeri accidentale, modificări accidentale ale informaţiilor. Pentru soluţionarea acestui tip de pierdere de date este suficienta menţinerea măcar a unei copii a datelor, într-un loc diferit de cel curent, pe un alt calculator, pentru protecţia lor.

2. Dezastre care afectează computerele ca întreg: incendii, inundaţii, cutremure. În cazul distrugerii componentelor hardware ale sistemului informatic, este necesar a se recupera datele de pe un suport aflat într-o zona de suficientă protecţie împotriva cauzelor generatoare ale dezastrului, cum ar fi un Seif rezistent la foc, o zona blindată sau o zonă aflată la o distanţă suficient de mare de locul de amplasare al calculatoarelor afectate. Pentru soluţionarea acestui tip de pierdere informaţiile se vor salva periodic (săptămânal, lunar) pe suport optic (CD,DVD) şi aceşti suporţi se vor depozita într-o zonă care poate să ofere protecţie la eventualele dezastre ce ar afecta partea hardware a computerelor.

- În cazul producerii unor astfel de dezastre ar putea exista 2 etape de recuperare, şi anume:

1. recuperarea funcţionalităţii sistemului prin înlocuirea pieselor defecte sau distruse, reinstalarea sistemului de operare şi a aplicaţiilor folosite de acel sistem;
2. restaurarea datelor pe suportul lor original de pe suportul lor de rezervă stocat în zona protejată (seif, încăpere blindată, altă zonă)

Informaticianul este responsabilul IT din unitatea şcolară.

- Informaticianul este angajat al unităţii, împuternicit să urmărească efectiv standardele de siguranţă şi să implementeze procedurile de siguranţă. Informaticianul are roluri şi responsabilităţi bine definite cu obiective clare in fisa postului sau in contract.

Responsabilităţile generale ale Informaticianului

- Informaticianul va participa la întocmirea procedurilor pentru prevenirea, detectarea, oprirea şi recuperarea datelor în urma atacurilor informaţionale din surse interne. Informaticianul trebuie să se asigure că aceste proceduri sunt respectate.
- Pentru implementarea cu succes a acestor proceduri este nevoie de asistenţă în ceea ce priveşte personalul şi fondurile astfel încât programele şi proiectele de siguranţă pot fi planificate şi executate în mod eficient.

Informaticianul are următoarele responsabilităţi majore:

- Recomandă strategii de siguranţă.
- Se asigură că procedurile de siguranţă sunt implementate pentru protecţia bunurilor informaţionale ale unitatii.
- Participă la revizuirea acestor proceduri.
- Actualizează sistemele de siguranţă informaţionale.

- În cadrul rolului său ca ofiţer responsabil cu siguranţa, Informaticianul trebuie să:
  - Înfiinţeze legături cu personalul responsabil cu securitatea datelor din toate compartimentele unitatii si cu cele din exteriorul unitatii cu care aceasta are diferite legaturi.
  - Se asigure că modelul de siguranţă IT este comunicat la cel mai înalt nivel si că planul de siguranţă beneficiază de susţinere din partea managementului.

- Pe lângă altele, Informaticianul este:
  - Responsabil cu dezvoltarea, implementarea şi revizuirea procedurii de securitate IT.
  - Implicat în procesul de luare a deciziilor cu privire la proiectarea, planificarea, achiziţionarea şi actualizarea tehnologiilor.
  - Reprezentantul pe probleme de securitate IT.
  - Persoana de contact pe probleme de securitate IT, cum ar fi întrebări, alerte, viruşi şi atacuri informaţionale.
  - Informează Şeful ierarhic cu privire la activităţile de siguranţă IT şi posibilele riscuri.

DERULAREA ACTIVITĂŢILOR

Principii generale de siguranţă

- Procesul de securizare a activităţii legate de domeniul I.T. consta in luarea unor măsuri de precauţie în momentul implicării în activităţi informaţionale pentru a asigura protecţia informaţiilor împotriva accesării, modificării, distrugerii sau publicării neautorizate.

Dotarea pe linie de IT

- Dotarea pe linie de I.T. trebuie sa constituie o preocupare permanentă a ofiţerului I.T. atât pentru a asigura buna întreţinere a echipamentelor existente cât şi pentru dezvoltarea infrastructurii şi achiziţia de tehnică de calcul nouă în concordanţă cu evoluţiile şi cerinţele din acest domeniu.
- Lista echipamentelor şi accesoriilor care fac obiectul acestei proceduri, fiind supusă modificărilor repetate este data ca anexă la procedură. De asemenea tot acolo este prezentată şi schema reţelei de calculatoare.

Moduri de introducere a informaţiilor în sistem

- Pentru a introduce informaţiile pe sistemele informatice, există mai multe căi, ce trebuie supravegheate pentru a asigura corectitudinea şi integritatea datelor. Aceste sunt:

- Introducerea de la tastatură: De la tastatură se pot introduce informaţii text pentru completarea documentelor. Această activitate reprezintă responsabilitatea operatorului, el fiind autorul şi responsabilul cu conţinutul astfel introdus.

- Introducerea datelor cu ajutorul scanerului. Informaţii atât în format grafic cât şi în format text pot fi introduse în calculator cu ajutorul scanerului. Responsabilitatea asupra conţinutului lor revine de asemenea operatorului şi ca şi în cazul precedent nu există pericole de a se introduce viruşi informatici sau a se deschide căi de atac informatic

- Introducerea de pe medii de stocare externă: CD, DVD, Dischetă, USB Flash Pen. Aceste moduri de introducerea a informaţiei reprezintă un grad crescut de risc, deoarece mediul lor sursă poate fi infectat cu anumiţi viruşi. De aceea se recomandă scanarea cu antivirusul local a informaţiilor ce urmează a fi introduse astfel în calculator.

- Primirea pe e-mail sau preluarea de pe pagini WEB a informaţiilor prezintă un grad sporit de risc faţă de mediile de stocare externe, deoarece, pe lângă viruşi informatici, împreună cu aceste se pot deschide căi de atac ale unui utilizator extern firmei, cum ar fi un hacker, bazat pe folosirea de troieni, viermi informatici, utilitare backdoor şi rootkit-uri. (pentru informaţii detaliate asupra acestor ameninţări a se vedea anexa cu descrierea lor detaliată). Pentru prevenirea unor astfel de riscuri, utilizatórul are datoria de a scana mesajele primite cu un program antivirus, sa nu acceseze mesaje, sau link-uri la pagini de WEB asupra cărora există dubii privind siguranţa lor. Sa dea acces din firewall-ul sistemului antivirus propriu pentru programe cookie sau pop-up de pe diverse situri web, doar daca s-a încredinţat de buna intenţie a respectivelor locaţii de internet.

Protecţie împotriva viruşilor

- Este foarte importantă adoptarea măsurilor de precauţie împotriva viruşilor pentru protecţia calculatoarelor şi datelor de pe acestea.
- Toate informaţiile descărcate de pe servere exterioare trebuie scanate imediat împotriva viruşilor utilizând aplicaţia anti-virus avizată de Informaticianul.
- Listele de viruşi continuă să crească în fiecare zi. Prin urmare este imperativă implementarea unui sistem automat de protecţie împotriva viruşilor. Se va alege un program anti-virus comercial proiectat pentru Windows. Toate programele sunt actualizate regulat.

Protecţia împotriva accesului extern neautorizat la informaţiile şi resursele I.T.

- Există situri de internet care pentru a putea fi vizualizate şi parcurse de către utilizator, necesită copierea pe calculatorul local al unor componente cookie.

- Acestea permit afişarea unor meniuri complexe de selecţie ale sitului, dar de asemenea permit spionarea informaţiilor de pe calculator respectiv scurgerea de informaţii şi de asemenea folosirea calculatorului în scopuri străine intereselor unitatii, cum ar fi: file sharing, participarea la diverse proiecte cu folosirea puterii de calcul a procesorului.
- În mod implicit copierea şi funcţionarea acestor componente este blocată de programul firewall instalat pe fiecare calculator.
- De aceea se recomandă utilizatorilor să permită selectiv şi cu precauţie funcţionarea acestor elemente cookie, prin permiterea accesului acestora doar pentru siturile sigure de internet, situri guvernamentale, ale furnizorilor de echipamente şi materiale.
- Este indicat, dacă este posibil, să nu se folosească deloc aceste componente cookie.

Managementul parolelor

- Fiecare calculator din cadrul reţelei interne trebuie să aibă o parolă de acces. Conturile şi parolele de utilizator sunt informaţii confidenţiale cunoscute doar de utilizatori.
- Următoarele principii se aplică în cadrul managementului parolelor:
  - Conturile Guest ale fiecărui calculator trebuie dezactivate.
  - Conturile Administrator ale fiecărui calculator în parte vor fi redenumite şi li se for atribui o parolă specială cunoscută doar Ofiţerului I.T.
  - Parolele trebuie să conţină cel puţin 8 caractere.
  - Parolele nu se împrumută. Dacă din anume motive un utilizator trebuie să dea parola altcuiva, parola trebuie schimbată imediat.
  - Parolele trebuie schimbate la 30 de zile.
  - Niciodată nu se trimite parola prin e-mail.
  - Parolele vechi şi parolele noi sunt scrise în formularul anexat pentru parole, împreună cu numele de utilizator şi numărul de identificare a calculatoarelor;
  - Trebuie setate screen-savere cu protecţie prin parolă. Screen-saverele trebuie să se activeze după 10 minute de inactivitate şi să solicite o parolă pentru accesarea sistemului de operare.
  - Parolele sunt înregistrate în formularul de evidenţe parole (vezi anexa) care va fi ţinut încuiat la şeful compartimentului în subordinea căruia se află utilizatorul.

Folosire neautorizată:

- Se consideră ca neacceptabilă orice activitate care:
  - Caută să folosească serviciile IT pentru probleme personale sau private.
  - Caută să obţină accesul neautorizat asupra resurselor unitatii.

- Întrerupe activitatea şi/sau serviciile reţelei.
- Iroseşte resurse (personal, capacitate şi calculatoare) prin aceste acţiuni.
- Distruge integritatea sau sustrage bunuri informaţionale.
- Compromite informaţiile .

- Informaticianul îşi rezervă dreptul să monitorizeze activităţile reţelei şi serviciilor acesteia.

Integritate fizică - Consideraţii generale

- Sistemul de calculatoare trebuie să fie protejat împotriva activităţilor negative externe şi interne. În general această protecţie constă în amplasarea calculatorului într-o încăpere închisă şi protejată împotriva accesului neautorizat.

- De asemenea, datorită fluctuaţiilor de curent din reţeaua electrică, care pot şi au dus în trecut la defectarea calculatoarelor s-a luat măsura achiziţiei surse neintreruptibile de tensiune si de prelungitoare cu protecţie la şocuri electrice, şi se recomandă ca, în afara orelor de program, calculatoarele să fie decuplate, pe cât posibil, de la reţeaua electrică.

Folosirea e-mail-ului

- Un alt aspect important pentru siguranţă este folosirea corectă a e-mailului.
- Utilizatorii trebuie să înţeleagă pe deplin riscurile implicate în trimiterea unui e-mail.
- In cadrul unitatii e-mail-urile ar trebui transmise cu aprobarea Şefului după ce au fost scanate de viruşi în prealabil.
- Este interzisă transmiterea de e-mailuri în interes personal.
- De asemenea responsabilitatea pentru conţinutul e-mail-urilor revine autorilor acestora, respectiv titularilor căsuţelor de e-mail.

Deschiderea ataşamentelor necunoscute

- Ataşamentele pot conţine viruşi sau coduri ascunse ce pot dezvălui parole sau deteriora informaţii deţinute.
- Nu se vor deschide e-mail-urile cu ataşamente sau din surse (având emitenţi) necunoscuti.
- Aceste mail-uri vor fi semnalate informaticianului, în timp util pt. ca acesta să poată lua măsurile adecvate de protecţie atât împotriva viruşilor/viermilor (programe dăunătoare sistemului) cât şi împotriva SPAM-ului (informaţii balast pt. sistem)

Salvarea datelor

- Pentru protecţia datelor importante ca şi pentru recuperarea lor în caz de dezastru se va efectua salvarea acestora utilizând un program pentru inscripţionarea acestora pe câte 2 CD-uri în mai multe sesiuni, o dată pe lună.
- Din raţiuni practice această activitate se va desfăşura lunar.

- CD-urile se vor încheia la sfârşitul lunii (salvările efectuate lunar) se vor pune în 2 plicuri sigilate, din care unul va rămâne la autor iar celalalt va fi predat pentru arhivare Informaticianului.
- Depozitarea acestora se va face în dulapul metalic al compartimentului I.T. pentru copia de siguranţă aflată acolo, respectiv într-un dulap securizat la efracţie pentru copia care rămâne la autor.
- În cazul în care din raţiuni practice va deveni fezabila şi necesară o salvare zilnică a datelor, se va proceda de maniera următoare: în fiecare zi la încheierea programului se vor salva pe o unitate externă (vezi tabelul următor) datele descrise în tabelul anterior, într-un singur exemplar, exemplar care va rămâne la autor, urmând ca după sfârşitul săptămânii (lunea din săptămâna următoare) aceste date sa fie salvate pe câte 2 CD cu sesiunea închisă, care se vor pune în plicuri sigilate din care unul va rămâne la autor iar unul va fi predat informaticianului spre arhivare.
- Pentru desfăşurarea în bune condiţii a acestor salvări, responsabilii cu acestea vor fi instruiţi periodic asupra modalităţilor hard şi soft de inscripţionare şi păstrare a datelor.
- Modul de realizare se va realiza inscripţionarea CD-urilor este descris în anexa 2 la această procedură iar salvările astfel efectuate se vor înregistra în formularul evidenţe salvări date (vezi anexa)

5.4.3. Valorificarea rezultatelor activităţii:

Rezultatele activității vor fi valorificate de Secretarul UAT şi toate compartimentele din Instituție.

6. Responsabilităţi şi răspunderi în derularea activităţii

1. Conducătorul instituției
- Aprobă procedura
- Asigură implementarea şi menținerea procedurii.

2. Preşedintele Comisiei SCIM
- Asigură implementarea şi menținerea prezentei proceduri;
- Monitorizează procedura

3. Informaticianul (responsabilul IT)

- Aplică și menține procedura;
- Realizează activitățile descrise la termenele stabilite în prezenta procedură
- Gestioneaza activitatile legate de cercetarea disciplinara

4. Conducătorii de compartimente/persoanele desemnate

- Aplică și mențin procedura;
- Realizează activitățile descrise la termenele stabilite în prezenta procedură

Indicatori de evaluare a eficienţei activităţii:

- Ponderea bazelor de date protejate în totalul bazelor de date (semestru/an):

(Număr baze de date protejate / Număr total baze de date) X 100

- Ponderea stațiilor de lucru protejate în totalul stațiilor de lucru (semestru/an):

(Număr stații de lucru protejate / Număr total stații de lucru) X 100

7. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii de sistem

Nr. Crt.	Ediţia sau, după caz , reviza ia în cadrul ediţiei	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediţiei sau reviziei ediţiei
1	2	3	4	5
7.1	Editia a III-a	-Legislatie primara -Legislatie secundara	Modificari legislative (conform Ordinului 600/2018)	05.07.2018
7.2	Editia a III-a Revizia I	Legislatie primara - Legislatie secundara	Modificari legislative(conform Ordinului 1054/2019)	24.11.2021

8. Formular de analiză a procedurii

Nr. Crt.	Compartiment	Nume şi prenume	Aviz	Data	Observaţii	Semnătura
1	2	3	4	5	6	7
1	Consiliu de Administratie	Orban Laura	Favorabil	24.11.2021		
2	Consiliul Profesoral	Pellegrini Lilla	Favorabil	24.11.2021		
3	Resurse Umane	Iacob Gabriela	Favorabil	24.11.2021		
4	Secretariat	Iacob Gabriela	Favorabil	24.11.2021		
5	Management	Pellegrini Lilla	Favorabil	24.11.2021		
6	Contabilitate	Vinersar Irina	Favorabil	24.11.2021		
7	CEAC	Balaci Otilia	Favorabil	24.11.2021		
8	Administrativ	Szabo Iosif	Favorabil	24.11.2021		
9	Comisie Monitorizare	Lădariu Diana	Favorabil	24.11.2021		

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

Nr. Crt.	Scopul difuzări	Ex. nr	Compartiment	Funcţia	Nume şi prenume	Data primirii	Data retragerii procedurii inlocuite	Data intrarii in vigoare	Semnatura
1	2	3	4	5	6	7	8	9	10
1	Aplicare, Evidența, Arhivare	1	Secretariat	Secretar Sef	Iacob Gabriela	24.11.2021	24.11.2021	24.11.2021	
2	Aplicare, Informare	2	Comisie Monitorizare	Responsabil Comisie Monitorizare	Lădariu Diana	24.11.2021	24.11.2021	24.11.2021	
3	Aplicare, Informare	3	Administrativ	Administrator	Szabo Iosif	24.11.2021	24.11.2021	24.11.2021	
4	Aplicare, Informare	4	Consiliu de Administratie	Membru Consiliu de Administrație	Orban Laura	24.11.2021	24.11.2021	24.11.2021	

Anexe, înregistrări, arhivări

- Toate documentele şi dovezile pe baza cărora se realizează activitatea procedurată se află în dosarele Comisiei SCIM, în dosarul Secretarului UAT şi în documentele echipei manageriale.
- Analiza şi revizuirea procedurii se face anual, sau ori de câte ori apar modificări ale reglementărilor legale cu caracter general şi intern pe baza cărora se desfăşoară activitatea care face obiectul acestei proceduri.