



**Republica Moldova**

**GUVERNUL**

**HOTĂRÎRE Nr. \_\_\_\_**  
**din \_\_\_\_\_.2020**

**cu privire la aprobarea Conceptului Sistemului Informațional de Management în Educație și a Regulamentului privind utilizarea și administrarea Sistemului Informațional de Management în Educație**

În temeiul art.157 lit.c) din Codul educației al Republicii Moldova nr.152/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr.319–324, art.634), cu modificările ulterioare, art.22 pct.3) lit.a) din Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6–12, art.44), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se aprobă:
  - 1) Conceptul Sistemului Informațional de Management în Educație, conform anexei nr.1;
  - 2) Regulamentul privind utilizarea și administrarea Modulului Învățământ primar, gimnazial și liceal al Sistemului Informațional de Management în Educație, conform anexei nr.2.
  - 3) Regulamentul privind utilizarea și administrarea Modulului Educație Timpurie al Sistemului Informațional de Management în Educație, conform anexei nr. 3.
2. Se instituie Sistemul Informațional de Management în Educație, proprietate a statului.
3. Se desemnează Ministerul Educației, Culturii și Cercetării, în calitate de posesor al Sistemului Informațional de Management în Educație.
4. Centrul Tehnologii Informaționale și Comunicaționale în Educație va asigura administrarea și dezvoltarea Sistemului Informațional de Management în Educație.
5. Serviciul Tehnologie Informației și Securitate Cibernetică, în calitate de posesor al platformei tehnologice guvernamentale comune (MCloud), va asigura gestiunea tehnico-tehnologică și mentenanța Sistemului Informațional de Management în Educație.
6. Se abrogă:
  - 1) Hotărârea Guvernului nr. 270/2007 cu privire la aprobarea Concepției sistemului informațional educațional (Monitorul Oficial al Republicii Moldova, 2007, nr. 51-53, art. 383).
  - 2) Hotărârea Guvernului nr. 899/2014 pentru aprobarea Regulamentului privind sistemul de cartografiere a școlilor primare, gimnaziilor și liceelor.
7. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Educației, Culturii și Cercetării.
8. Prezenta hotărâre intră în vigoare la data publicării.

**PRIM-MINISTRU**

**Ion CHICU**

**Contrasemnează:**

**Ministru al educației,  
culturii și cercetării**

**Igor ȘAROV**

## **CONCEPTUL** **Sistemului Informațional de Management în Educație**

### **Capitolul I** **DISPOZIȚII GENERALE**

1. Implementarea cu succes a reformelor în educație necesită elaborarea și implementarea unor noi mijloace automatizate de asigurare informațională a autorităților publice centrale și locale, instituțiilor de învățământ, organizațiilor societății civile, cetățenilor Republicii Moldova. Noile mijloace de asigurare informațională trebuie să corespundă atât noii structuri a sistemului de învățământ din Republica Moldova, cât și realizărilor de ultimă oră în domeniul tehnologiei informației și comunicațiilor.

2. Factorii principali, care determină oportunitatea elaborării unui sistem informațional automatizat modern al educației, sunt:

1) necesitatea înregistrării la nivel național a traseelor educaționale ale copiilor, elevilor și studenților în scopul prevenirii neșcolarizării, abandonului școlar și părăsirii premature a sistemului de învățământ obligatoriu;

2) necesitatea de a dispune la nivel național de informații referitoare la cerințele educaționale ale copiilor, elevilor și studenților în scopul planificării și implementării măsurilor ce asigură și garantează accesul universal la o educație de calitate, respectarea drepturilor omului;

3) necesitatea de a dispune la nivel național de informații referitoare la componenta și calificarea angajaților din sistemul de învățământ în scopul asigurării instituțiilor de învățământ cu cadre didactice, didactic-științifice și manageriale calificate, planificării și implementării măsurilor de atragere și menținere a cadrelor în învățământ, de pregătire inițială și continuă a specialiștilor în domeniul educației;

4) nevoia de date veridice și relevante despre infrastructura fiecărei instituții de învățământ, numărul de copii, elevi, studenți, după caz, de angajați ai instituțiilor de învățământ, necesare pentru planificarea bugetară, monitorizarea eficienței, corectitudinii și legalității utilizării mijloacelor alocate de către stat, prevenirii cazurilor de mistificări, deturnării de fonduri;

5) lipsa în prezent a unui suport informațional pentru planificarea și implementarea măsurilor de combatere a corupției în educație, în special, de acoperire a absenteismului, mistificării notelor, inflației de merite academice, falsificării actelor de studii;

6) lipsa în prezent a unui suport informațional pentru măsurarea performanțelor și efectuarea de clasamente ale instituțiilor de învățământ, colectarea și publicarea datelor deschise despre fiecare instituție de învățământ și sistemul de învățământ în ansamblu;

7) lipsa în prezent a unui suport informațional pentru constatarea cazurilor de gestionare defectuoasă a instituțiilor de învățământ din Republica Moldova.

3. Denumirea sistemului: Sistemul Informațional de Management în Educație (în continuare SIME).

4. Definiția sistemului:

SIME reprezintă totalitatea infrastructurii și resurselor informaționale, normelor juridice, structurilor organizatorice, destinată pentru asigurarea activității autorităților administrației publice centrale și locale în domeniul învățământului.

5. Locul sistemului în Spațiul informațional unic:

SIME este parte componentă a Resurselor informaționale de stat ale Republicii Moldova, segmentul "Evidența automatizată a resurselor asigurării sociale, deservirii medicale, educației și științei".

6. Noțiunile principale utilizate în prezenta Concepție au următoarea semnificație:

*deschiderea datelor* – publicarea de date oficiale ce conțin informații cu caracter statistic, structurate într-o listă sau într-o formă non-narativă, reprezentate în formate digitale non-proprietare ce pot fi procesate în mod automat;

*extensibilitate* – capacitatea sistemului de a realiza funcționalități noi în condițiile în care îi sunt adăugate resurse hardware și/sau software adiționale, fără a fi necesară schimbarea întregii infrastructuri informaționale;

*fișa instituției de învățământ* – document de format unitar ce conține date referitoare la performanțele academice, nivelul de calificare a cadrelor didactice, didactico-științifice și manageriale, executarea bugetelor anuale, serviciile educaționale oferite și locul instituției de învățământ în clasamentele naționale și, după caz, în unitățile administrativ-teritoriale;

*modularitate* – capacitatea părților componente ale sistemelor informatice de a funcționa independent, dar folosind baze de date comune, respectând caracteristica principală de mediu integrat;

registrator – entitatea responsabilă de introducerea și /sau actualizarea datelor în SIME.

#### 7. Destinația sistemului:

SIME este destinat pentru gestionarea datelor educaționale și oferirea tuturor celor interesați (autorități și instituții ale statului, instituții de învățământ, societatea civilă, cetățeni etc.) a informației actuale cu privire la domeniul educației în Republica Moldova și este format din următoarele module corespunzătoare tipurilor instituțiilor de învățământ.

Sistemul elaborat va servi ca instrument electronic eficient pentru analiza și planificarea strategică a politicilor educaționale, elaborarea și monitorizarea implementării reformelor pe domeniul educației, precum și identificarea cazurilor de abandon școlar, de părăsire prematură a sistemului de învățământ.

8. Scopul SIME este de a asigura Ministerul Educației, Culturii și Cercetării (MECC), alte autorități publice centrale, autorități publice locale și instituții de învățământ cu date actualizate privind sistemul educațional pentru elaborarea și implementarea politicilor educaționale, monitorizarea și evaluarea impactului acestora. Astfel, SIME va deveni unica sursă de date veridice cu referire la sistemul educațional.

#### 9. Obiectivele SIME sunt:

1) Modernizarea managementului educațional prin consolidarea capacităților MECC, administrațiilor publice locale și ale instituțiilor de învățământ de colectare, stocare, prelucrare, transmitere și deschidere a datelor din domeniul educației.

2) Eficientizarea gestionării de către MECC autoritățile publice locale și instituțiile de învățământ a finanțelor publice destinate sistemului educațional.

3) Sporirea validității și accesibilității datelor din domeniul educației și asigurarea plenitudinii acestora, în limitele legislației cu privire la protecția datelor cu caracter personal.

4) Asigurarea transparenței decizionale din sistemul educațional prin digitalizarea proceselor din sistem și deschiderea datelor statistice din domeniul educației pentru societatea civilă.

5) Ținerea evidenței unice centralizate a instituțiilor de învățământ, organelor locale de specialitate în domeniul învățământului, copiilor, elevilor, studenților, cadrelor didactice, actelor de studii și a calificărilor în scopul creării condițiilor pentru prevenirea abandonului școlar și părăsirea prematură a sistemului de învățământ, identificarea cazurilor de falsificare a actelor oficiale și optimizarea utilizării bunurilor materiale și mijloacelor financiare alocate de către stat.

#### 10. Sarcinile de bază ale SIME sunt:

1) Asigurarea autorităților administrației publice de competență cu informații veridice și operative privind domeniul educației.

2) Asigurarea interacțiunii eficiente între ministere și alte autorități ale administrației publice interesate.

3) Asigurarea evidenței copiilor, elevilor și studenților în scopul prevenirii neșcolarizării, abandonului școlar și părăsirii premature a sistemului de învățământ.

4) Controlul măsurilor aplicate pentru diminuarea neșcolarizării, abandonului școlar și părăsirea premature a sistemului de învățământ.

5) Asigurarea evidenței angajaților instituțiilor de învățământ în scopul asigurării cerințelor legale referitoare la angajarea, promovarea și formarea continuă a cadrelor didactice și manageriale.

6) Controlul practic al măsurilor aplicate pentru respectarea legislației și eficienței politicilor de atragere, angajare, promovare și formare continuă a cadrelor didactice, științifico-didactice și manageriale.

7) Asigurarea evidenței instituțiilor de învățământ în scopul planificării strategice a educației, dezvoltării rețelei de instituții de învățământ, garantării accesului la educație, clasamentul instituțiilor de învățământ în funcție de performanțele academice, eficacitate și eficiență.

8) Controlul practic al măsurilor aplicate pentru garantarea accesului la o educație de calitate, creării condițiilor pentru dezvoltarea școlilor prietenoase copilului.

9) Automatizarea fluxurilor de date ce țin de monitorizarea și evaluarea sistemului educațional.

10) Structurarea clară și uniformă a informației din domeniul educației, asigurarea compatibilității metadatelor din învățământ cu standardele naționale și internaționale.

11) Excluderea dublării informațiilor prin preluarea on-line a datelor statistice primare direct din instituțiile de învățământ și organele locale de specialitate din domeniul învățământului, utilizarea largă a resurselor informaționale administrative.

12) Asigurarea informațională a activității de analiză, prognozare și cercetare în domeniul educației.

13) Asigurarea cu instrumentarul statistic necesar pentru elaborarea, implementarea, monitorizarea și evaluarea impactului politicilor educaționale.

14) Asigurarea vizualizării informației stocate (cu diferite niveluri de acces) și generarea, salvarea și editarea rapoartelor predefinite și specifice.

15) Deschiderea datelor din domeniul educației prin publicarea acestora pe Portalul datelor deschise al SIME.

16) Accesarea rapidă, garantată a datelor publice și informației despre sistemul educațional și instituțiile de învățământ, indiferent de locație.

11. Principiile de bază ale SIME sunt:

1) *principiul legitimității*, conform căruia funcționalitățile oferite utilizatorilor și operațiile efectuate de ei trebuie să fie legale și conforme cu drepturile omului și legislația națională în vigoare;

2) *principiul transparenței*, care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de SIME;

3) *principiul autenticității datelor*, care presupune că informațiile păstrate pe dispozitivele de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor din SIME;

4) *principiul identificării*, potrivit căruia pachetelor informaționale li se atribuie un cod de clasificare la nivel de sistem, prin care este asigurată identificarea univocă a acestora și raportarea la acestea;

5) *principiul temeiniciei datelor*, care prevede că introducerea datelor în SIME se efectuează doar în baza înscrisurilor din documentele acceptate ca surse de informații;

6) *principiul auditului sistemului*, care presupune înregistrarea informației despre schimbările ce au loc, pentru a face posibilă reconstituirea istoriei unui obiect sau starea lui la o etapă anterioară;

7) *principiul accesibilității și interoperabilității*, care presupune că SIME, chiar dacă oferă funcționalități multiple, este construit ca un element integral și folosit de utilizatori prin intermediul unei interfețe unice. Mai mult decât atât, acest principiu prevede că extinderea și dezvoltarea sistemului se vor face prin protocoale și puncte de conexiune proiectate din start;

8) *principiul confidențialității informației*, care prevede răspunderea personală, în conformitate cu legislația în vigoare, a utilizatorilor responsabili de introducerea, prelucrarea și accesarea informației din sistem pentru folosirea și utilizarea neautorizată a informației;

9) *principiul compatibilității*, conform căruia SIME trebuie să fie compatibil cu sistemele existente atât în țară, cât și peste hotarele ei;

10) *principiul stabilității*, care constă în capacitatea sistemului de a funcționa eficient în condițiile modificării cadrului legislativ;

11) *principiul orientării spre utilizator*, potrivit căruia structura, conținutul, mijloacele de acces și navigarea sunt focalizate spre utilizatori;

12) *principiul utilizării standardelor deschise*, care se va aplica pentru a asigura atât interoperabilitatea cu sisteme existente, cât și păstrarea informației, în conformitate cu normele în vigoare;

13) *principiul securității informației*, care presupune garantarea nivelului prestabilit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirii pentru lucru atât a SIME, cât și a datelor acestuia.

14) *principiul divizării arhitecturii pe niveluri*, fapt ce va permite efectuarea proiectării și dezvoltării independente a contururilor funcționale ale SIME, în conformitate cu standardele de interfață dintre niveluri;

15) *principiul modularității*, care reprezintă posibilitatea dezvoltării sistemului fără modificarea componentelor create anterior;

16) *principiul adaptabilității și flexibilității sistemului*, care asigură posibilitatea de a modifica configurația SIME fără eforturi suplimentare de programare pentru rezolvarea problemelor noi și pentru funcționare în condiții și regimuri în schimbare;

17) *principiul extensibilității*, conform căruia va fi garantată posibilitatea extinderii și completării SIME cu noi funcții sau îmbunătățirea celor existente;

18) *principiul scalabilității*, conform căruia, odată cu creșterea volumului de date și a solicitării sistemului informatic, performanțele SIME nu se vor diminua;

19) *principiul dezvoltării progresive*, potrivit căruia elaborarea sistemului și modernizarea permanentă a componentelor sale se va efectua în conformitate cu avansarea tehnologiei informației și a comunicațiilor;

20) *principiul consecutivității*, care presupune elaborarea și implementarea SIME pe etape;

21) *principiul eficienței funcționării*, care presupune optimizarea raportului dintre calitate și cost;

22) *principiul independenței de platforma software*, conform căruia SIME poate fi construit pe baza modulelor elaborate la comandă sau a produselor software existente. Concepția nu limitează în nici un fel metodele de dezvoltare a sistemului atât timp cât sunt satisfăcute nevoile indicate și se oferă cea mai mare valoare pentru prețul oferit;

23) *principiul primei persoane/ centrului unic*, care presupune existența unei entități de conducere efectivă de rang superior, care are competente și abilități suficiente pentru luarea deciziilor și coordonarea lucrărilor de creare și exploatare a SIME;

24) *principiul controlului asupra dezvoltării și utilizării SIME*, care se exercită prin intermediul unui șir de măsuri tehnico-organizaționale și aplicații de program, menite să asigure calitatea înaltă a resurselor informaționale de stat, gradul maxim de siguranță a păstrării și gestionării lor, inclusiv corectitudinea utilizării acestora conform standardelor prevăzute de legislația în vigoare.

## **Capitolul II**

### **CADRUL DE REGLEMENTARE AL SIME**

12. Cadrul de reglementare al SIME corespunde legislației naționale în vigoare, tratatelor și convențiilor internaționale la care Republica Moldova este parte:

- 1) Constituția Republicii Moldova.
- 2) Codul Educației nr. 152 din 17.07.2014.
- 3) Legea nr. 338 din 15.12.1994 cu privire la drepturile copilului.
- 4) Legea nr. 982 din 11.05.2000 privind accesul la informație.
- 5) Legea nr. 467 din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat.
- 6) Legea nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic.
- 7) Legea nr. 71 din 22.03.2007 cu privire la registre.
- 8) Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.
- 9) Legea nr. 140 din 14.06.2013 privind protecția specială a copiilor aflați în situație de risc și a copiilor separați de părinți.
- 10) Legea nr. 60 din 30.03.2012 privind incluziunea socială a persoanelor cu dizabilități.
- 11) Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate.
- 12) Hotărârea Guvernului nr. 733 din 28.06.2006 "Cu privire la Concepția guvernării electronice".

13) Hotărârea Guvernului nr. 653 din 06.11.2009 „Cu privire la aprobarea Regulamentului, structurii și efectivului-limită ale aparatului central al Ministerului Educației”.

14) Hotărârea Guvernului nr. 1123 din 14.12.2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”.

15) Hotărârea Guvernului nr. 523 din 11.07.2011 „Cu privire la aprobarea Programului de dezvoltare a educației incluzive în Republica Moldova pentru anii 2011-2020”.

16) Hotărârea Guvernului nr. 414 din 08.05.2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.

17) Hotărârea Guvernului nr. 710 din 20.09.2011 „Cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare)”.

18) Hotărârea Guvernului nr. 656 din 05.09.2012 „Cu privire la aprobarea Programului privind Cadrul de Interoperabilitate”;

19) Hotărârea Guvernului nr. 211/2019 „Privind platforma de interoperabilitate (MConnect)”.

20) Hotărârea Guvernului nr. 1090 din 31.12.2013 „Privind serviciul electronic guvernamental de autentificare și control al accesului (MPass)”.

21) Hotărârea Guvernului nr. 128 din 20.02.2014 „Privind platforma tehnologică guvernamentală comună (MCloud)”.

22) Hotărârea Guvernului nr. 405 din 02.06.2014 „Privind serviciul electronic guvernamental integrat de semnătură digitală (MSign)”.

23) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog).

24) Hotărârea Guvernului nr. 434 din 20.06.2014 „Privind aprobarea Strategiei pentru protecția copilului pe anii 2014-2020”.

25) Hotărârea Guvernului nr. 717 din 29.08.2014 „Privind platforma guvernamentală de registre și acte permissive (PGRAP)”.

26) Hotărârea Guvernului nr. 944 din 14.11.2014 „Cu privire la aprobarea Strategiei de dezvoltare a educației pentru anii 2014-2020 „Educația - 2020”.

27) Hotărârea Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică.

28) Ordinul Ministerului Dezvoltării Informaționale nr. 78 din 01.06.2006 “Cu privire la aprobarea reglementării tehnice "Procese ciclului de viață al software-ului”.

### **Capitolul III**

#### **SPAȚIUL FUNCȚIONAL AL SIME**

13. Funcțiile ale SIME sunt:

1) formarea bazei de date a sistemului informațional automatizat de management în educație;

2) identificarea și luarea la evidență a persoanelor juridice și fizice din domeniul educațional;

3) actualizarea datelor despre entitățile de evidență prin completarea și modificarea atributelor obiectelor informaționale;

4) radierea din evidență a entităților din domeniul educației prin modificarea statutului obiectelor informaționale corespunzătoare;

5) organizarea asigurării informaționale prin oferirea accesului la datele din SIME tuturor autorităților și instituțiilor implicate în procesele de înregistrare, modificare și radiere a entităților din domeniul educației, în conformitate cu legislația și competențele atribuite acestora;

6) asigurarea fluxurilor de date și a mecanismelor de control asupra lor;

7) asigurarea interacțiunii SIME cu alte sisteme informaționale. Schimbul de informații cu alte sisteme automatizate se realizează conform cadrului normativ cu privire la schimbul de date și interoperabilitate ;

8) asigurarea veridicității, integrității, calității și plenitudinii datelor la toate etapele de colectare, stocare, transmitere și prezentare;

9) asigurarea protecției datelor și securității acestora la toate etapele de acumulare, păstrare, prelucrare, transmitere și utilizare a resurselor informaționale de stat;

10) asigurarea autorităților competente ale administrației publice și a publicului cu informație relevantă;

11) generarea rapoartelor statistice și analitice pentru prezentarea către autoritățile publice centrale și locale, persoanele fizice și juridice în conformitate cu legislația în vigoare a Republicii Moldova;

12) publicarea datelor deschise despre fiecare instituție de învățământ și domeniul educației în ansamblu;

13) furnizarea datelor pentru prestarea serviciilor digitale din domeniul educației;

14) asigurarea multilaterală și multidimensională a funcționării SIME și integrării cu alte sisteme informaționale;

15) asigurarea autentificării și autorizării utilizatorilor;

16) asigurarea administrării și configurării parametrilor sistemului în conformitate cu evoluția domeniului educației.

14. Reieșind din funcțiile SIME, sistemul va avea următoarele contururi de bază:

1) Evidența instituțiilor de învățământ.

2) Evidența entităților ce prestează servicii de formare continuă.

3) Evidența organelor locale de specialitate în domeniul învățământului.

4) Evidența calificărilor.

15. Contururile funcționale includ următoarele funcții:

1) evidența instituțiilor de învățământ general, profesional tehnic, superioare și de formare continuă;

2) evidența copiilor, elevilor, studenților și cursanților;

3) evidența reușitei academice zilnice;

4) evidența angajaților instituțiilor de învățământ;

5) identificarea persoanelor de vârstă învățământului obligatoriu ce nu sunt cuprinse în nici o formă de învățământ sau au abandonat prematur studiile;

6) evidența organelor locale de specialitate în domeniul învățământului;

7) producerea de rapoarte statistice privind starea învățământului la nivel de instituții, unități teritorial administrative, regionale, în ansamblu pe țară.

16. Conturul de evidență automatizată a calificărilor include următoarele funcții:

1) evidența calificărilor;

2) producerea de rapoarte statistice referitoare la calificări.

17. SIME va face schimb de date, prin intermediul platformei de interoperabilitate (MConnect) cu următoarele sisteme informaționale automatizate:

1) Registrul de stat al populației.

2) Registrul de stat al unităților de drept.

3) Alte registre de Stat accesibile pentru schimbul de date.

SIME va fi integrat și va reutiliza serviciile electronice guvernamentale de platformă existente:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul SIME și a registrelor formate de acesta, utilizând diverse metode de autentificare (semnătură electronică, semnătură mobilă, buletinul de identitate electronic);

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice în cadrul utilizării SIME și a registrelor formate de acesta;

3) serviciul electronic guvernamental de jurnalizare (MLog) – instrument securizat și flexibil de jurnalizare și audit, utilizat pentru asigurarea evidenței operațiunilor (evenimentelor) produse în SIME și registrele formate de acesta.

## **Capitolul IV**

### **STRUCTURA ORGANIZAȚIONALĂ A SISTEMULUI**

18. Părțile implicate în implementarea și utilizarea SIME:

1) Proprietar al SIME este statul.

2) Posesor al SIME este MECCa Republicii Moldova.

3) Deținător al SIME este Centrul de Tehnologii Informaționale și Comunicaționale (CTICE) din subordinea MECC a Republicii Moldova.

4) Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC), în calitate de posesor al platformei tehnologice guvernamentale comune (MCloud), va asigura gestiunea tehnico-tehnologică și mentenanța Sistemului Informațional de Management în Educație.

19. Sursele de informații ale sistemului sunt:

1) MECC a Republicii Moldova.

2) Instituțiile de învățământ.

3) Alte autorități publice centrale și locale care au în subordine instituții de învățământ.

4) Academia de Științe a Moldovei (ASM).

5) Agenția Națională de Asigurare a Calității în Educație și Cercetare (ANACEC).

6) Agenția Națională pentru Curriculum și Evaluare (ANCE) din subordinea MECC a Republicii Moldova.

7) CTICE din subordinea MECC a Republicii Moldova.

20. Registratori ai SIME sunt:

a) instituțiile de învățământ – înregistrează, actualizează, radiază datele despre instituții, clase, grupe, secții, elevi, angajați, utilizatori ai sistemului din cadrul instituțiilor de învățământ în cauză;

b) organele locale de specialitate în domeniul învățământului – înregistrează, actualizează, radiază datele despre organele de specialitate, rețeaua de instituții de învățământ din unitățile teritorial-administrative în cauză, angajații și utilizatorii sistemului din cadrul organelor de specialitate în cauză;

c) deținătorul SIME – înregistrează, actualizează, radiază datele despre rețeaua de instituții de învățământ aflate în subordinea MECC, altor organe ale administrației publice centrale, utilizatorii sistemului din cadrul administrației publice centrale.

21. Accesul la datele cu caracter personal pentru sistemele informaționale externe și utilizatorii externi va fi oferit cu consimțământul subiectului datelor cu caracter personal adult sau minor care este supus măsurii de ocrotire judiciare sub forma tutelei. Consimțământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentantul legal, în cazul minorului, sau de către tutore, în cazul adultului.

22. Posesorul și deținătorul asigură condițiile organizatorice și financiare pentru funcționarea SIME.

## **Capitolul V**

### **DOCUMENTELE SISTEMULUI**

23. În cadrul SIME se utilizează documente de intrare, documente împrumutate de la alte sisteme informaționale și documente de ieșire.

24. Documentele de intrare includ:

a) dosarele personale ale copiilor, elevilor, studenților, perfectate de către instituțiile de învățământ;

b) dosarele personale ale angajaților, perfectate de către instituțiile de învățământ, organele locale de specialitate în domeniul învățământului, alte instituții ce solicită accesul la datele din SIME;

c) registrele de grupă, clasă, cerc, secție;

d) registrele de evidență ale instituțiilor de învățământ;

e) rapoartele financiare anuale ale instituțiilor de învățământ;

f) documentația de proiect a clădirii/ clădirilor instituțiilor de învățământ;

g) deciziile autorităților publice locale referitoare la crearea, modificarea sau desființarea districtelor școlare;

h) ordinile ANCE referitoare la rezultatele evaluărilor naționale, concursurilor și olimpiadelor republicane și internaționale;

i) deciziile ANACEC referitoare la acreditare și evaluare;

j) actele de studii personalizate de către CTICE;

k) ordinele instituțiilor de învățământ, organelor locale de specialitate în domeniul învățământului, MECC privind acordarea, modificarea sau retragerea drepturilor de utilizator, conform competenței.

25. Documentele împrumutate de la alte sisteme informaționale includ:

- a) documentele de identificare a persoanelor;
- b) documentele de înregistrare a unităților de drept;
- c) licențele și autorizațiile de activitate;
- d) rapoartele și informațiile statistice.

26. Documentele de ieșire includ rapoarte analitice și statistice cu privire la:

- 1) instituțiile de învățământ;
- 2) elevi în instituțiile de învățământ;
- 3) studenți în instituțiile de învățământ;
- 4) absolvenți ai instituțiilor de învățământ;
- 5) angajați în instituțiile de învățământ;
- 6) angajați în organele locale de specialitate în domeniul învățământului;
- 7) școlarizarea;
- 8) abandonul școlar;
- 9) părăsirea prematură a învățământului;
- 10) bugetele anuale ale instituțiilor de învățământ;
- 11) infrastructura instituțiilor de învățământ;
- 12) calificări;
- 13) fișele instituțiilor de învățământ;
- 14) necesarul de cadre didactice în instituții de învățământ;
- 15) extrase privind listele copiilor/ elevilor ce au abandonat învățământul general obligatoriu din țară;

16) extrase privind listele elevilor/ studenților ce au abandonat prematur învățământul din țară;

17) extrase privind înmatricularea, durata studiilor, abandonul, exmatricularea, absolvirea instituțiilor de învățământ de către anumite persoane;

18) răspunsuri la interpelări, întocmite în baza informației din baza de date ale sistemului.

După caz, rapoartele analitice și statistice vor fi dezagregate pe tipuri de instituții de învățământ, unități teritorial-administrative, niveluri și cicluri de învățământ, limba de instruire, limba maternă, gen, situația socio-economică a cetățenilor, mediul de reședință.

## **Capitolul VI**

### **SPAȚIU INFORMAȚIONAL AL SISTEMULUI**

#### **Secțiunea 1. Obiectele informaționale gestionate de SIME**

27. Principalele obiecte informaționale ale SIME sunt:

1) Instituția de învățământ - obiect informațional generic care reprezintă persoanele juridice înregistrate prin numărul de identificare de stat al unității de drept (IDNO). Instituțiile de învățământ fără statut de personalitate juridică sunt înregistrate prin instituția de bază, raion, localitate, denumire. Caracteristicile obiectului informațional - instituția de învățământ:

- a) numărul de identificare de stat al instituției de învățământ (IDNO);
- b) codul unic de identificare a întreprinderilor și organizațiilor (CUIIO);
- c) codul trezoreria;
- d) codul fiscal;
- e) denumirea;
- f) fondator;
- g) adresa;
- h) telefon, fax, e-mail;
- i) categoria instituției;
- j) tipul instituției;
- k) acreditarea/ autorizarea provizorie de funcționare, după caz;
- l) structura instituției;

- m) numărul posturilor pentru fiecare categorie de personal;
- n) limba majoritară de comunicare în localitatea în care se află instituția;
- o) numărul de schimburi;
- p) anul ultimei reorganizări;
- q) modul de reorganizare;
- r) conducător (numele, prenumele, telefon, e-mail);
- s) programele de formare profesională oferite, după caz;
- t) rețeaua de grupe, clase, cercuri, secții sportive, după caz;
- u) infrastructura;
- v) alte date cu privire la instituția de învățământ;
- w) date despre resursele informaționale (manuale)

2) Copil/elev/student/cursant se identifică prin numărul de identificare al persoanei fizice (IDNP / alte acte de identificare). Caracteristicile obiectului informațional – copil / elev / student / cursant:

- a) codul numeric personal al persoanei fizice (IDNP);
- b) codul certificatului de naștere, codul actului de identitate, în lipsa IDNP, după caz;
- c) numele, prenumele;
- d) data nașterii;
- e) genul;
- f) adresa;
- g) telefonul;
- h) date despre părinți (numele, prenumele, date de contact);
- i) date despre instituția de învățământ în care este înscris (IDNO, CUIIO);
- j) date despre subdiviziunea structurală a cărei îi aparține;
- k) cetățenia, după caz;
- l) limba maternă, limba de instruire, limbile străine studiate, după caz;
- m) repetă anul, după caz;
- n) studiază limba maternă ca o disciplină distinctă;
- o) date despre copil / elev / student aflat în situație de risc (este instituită tutela / curatela; de

cine este exercitată tutela / curatela; situația de risc (orfan, monoparental, cu dezabilitate, trei sau mai mulți copii minori în familie, numărul de părinți șomeri în familie, familie fără venituri sau cu venituri mici, limba maternă nu coincide cu limba de instruire, numărul părinților plecați peste hotare); în grija cui a rămas persoana), după caz. Accesul la aceste date este limitat la nivel de instituție de învățământ.

p) date despre copil / elev / student cu cerințe educaționale speciale (instruirea la domiciliu; tulburări emoționale (afective) și de comportament; tulburări de limbaj; dificultăți de învățare; comportament deviant; întârziere/ dizabilitate mintală/ intelectuală/ dificultăți severe de învățare; dizabilități fizice/ neuromotorii; dizabilități de văz; deficiențe de auz; măsurile de intervenție; planul educațional și/sau de asistență; tipul planului educațional individualizat), după caz. Accesul la aceste date este limitat la nivel de instituție de învățământ.

- q) data înscrierii în această instituție;
- r) motivul venirii în această instituție, după caz;
- s) distanța de la locul de trai până la această instituție, după caz;
- t) modul în care copilul/elevul/studentul vine la această instituție, după caz;
- u) statutul copilului/elevului/studentul (înmătriculat, învață; înmatriculat, dar a abandonat studiile; exmatriculat);
- v) data orientativă a abandonului școlar, dacă este cazul;
- w) motivul abandonului școlar, după caz;
- x) data și motivul exmatriculării din această instituție;
- y) grupele/ cercurile/ secțiile pe care le frecventează;
- z) numărul de ore absente motivate / nemotivate, după caz;
- aa) planul-cadru / programul de formare profesională urmat, după caz;
- bb) ciclul de studii, după caz;
- cc) calificarea, după caz;
- dd) rezultatele și / sau situația academică;
- ee) date despre conectarea la domiciliu la Internet;

ff) date despre posesia dispozitivelor (gadgeturilor) la domiciliu conectate la internet.

3) Angajat al instituției de învățământ. Caracteristicile obiectului informațional – angajat al instituției de învățământ:

- a) codul numeric personal al persoanei fizice (IDNP);
- b) numele, prenumele;
- c) data nașterii;
- d) genul;
- e) categoria de personal (de conducere, didactic etc.);
- f) date despre instituția de învățământ în care este angajat (IDNO, CUIIO);
- g) data angajării;
- h) data concedierii, dacă este cazul;
- i) motivul concedierii, dacă este cazul;
- j) este stabilită pensia de vârstă;
- k) postul/funcția;
- l) modul de angajare (de bază, prin cumul etc.);
- m) durata contractului individual de muncă;
- n) nivelul de studii;
- o) studiile pedagogice / profesionale;
- p) gradul didactic / managerial / titlul științific/ titlul științifico-didactic, după caz;
- q) vechimea în muncă;
- r) vechimea în muncă în sectoarele reale ale economiei, după caz;
- s) nivelul grupelor/ claselor în care predă;
- t) volumul de muncă, după caz;
- u) disciplinele predate, după caz.
- v) date despre formarea continuă a angajatului, după caz.
- w) date despre conectarea la domiciliu la Internet;
- x) date despre posesia dispozitivelor (gadgeturilor) la domiciliu conectate la internet.

4) Subdiviziuni structurale (clase, grupe etc.) ale instituției de învățământ - sunt identificate prin identificatorul instituției și codul atribuit de instituția de învățământ în cauză. Caracteristicile obiectului informațional – subdiviziuni structurale ale instituției de învățământ:

a) identificatorul instituției și codul atribuit subdiviziunii structurale de către instituția de învățământ în cauză;

- b) denumirea;
- c) nivelul;
- d) profilul;
- e) statutul;
- f) limba de instruire;
- g) tipul planului de învățământ / calendarului academic, după caz;
- h) numărul de ore pe săptămână, după caz;
- i) schimbul.

5) Organ local de specialitate în domeniul învățământului secundar se identifică prin numărul de identificare de stat al unității de drept (IDNO).

6) Angajat al organului local de specialitate în domeniul învățământului.

7) Calificarea angajatului se identifică prin codul atribuit de Agenția Națională de Asigurare a Calității în Educație și Cercetare.

Caracteristicile obiectului informațional – calificarea angajatului:

a) codul/coduri atribuite calificării de către Agenția Națională de Asigurare a Calității în Educație și Cercetare:

- b) denumirea calificării (titlul de calificare profesională acordat);
- c) nivelul programului de formare profesională;
- d) domeniul general de studiu;
- e) domeniul de formare profesională;
- f) domeniul ocupațional;
- g) specialitatea / program de studiu.

8) Utilizator al sistemului obiect informațional generic care reprezintă orice utilizator al SIME. Caracteristicile obiectului informațional – utilizator al SIME:

- a) codul personal al persoanei fizice (IDNP);
- b) numele, prenumele;
- c) telefon, adresa de poștă electronică;
- d) rolul;
- e) data atribuirii statutului de utilizator;
- f) data expirării statutului de utilizator;
- g) date cu privire la modificarea parolei;
- h) data ultimei intrări reușite în sistem.

28. Posibilitățile utilizatorului depind de contextul în care el se află și rolul lui în sistem:

- 1) administrator național – are acces la toate informațiile din sistem;
- 2) administrator raional/municipal – are acces doar la datele referitoare la învățământul din unitatea teritorial-administrativă de care este responsabil;
- 3) administrator al instituției – are acces doar la datele referitoare la instituția de învățământ în care activează;
- 4) operator al subdiviziunii structurale – are acces doar la datele referitoare la subdiviziunea de care este responsabil (clasa, grupa etc.);
- 5) expert - operator al subdiviziunii structurale care are acces doar la datele referitoare la subdiviziunea de care este responsabil (clasa, grupa etc.) cu restricționarea de a modifica datele educaționale;
- 6) economist- are drepturile similare ca operatorul al subdiviziunii structurale cu accesul la datele economico-financiare;
- 7) analist raional/național/ instituție - are acces doar la vizualizarea datelor prin rapoartele accesibile;
- 8) angajat al instituției de formare continuă.

## **Secțiunea 2. Scenariile de bază aferente obiectelor informaționale**

29. Scenariul de bază reprezintă lista evenimentelor aferente obiectelor informaționale gestionate de sistem:

- 1) evidența obiectului se efectuează în baza ordinelor de înmatriculare, ordinelor cu privire la mișcarea personalului / copiilor / elevilor / studenților, ordinelor de desemnare în calitate de utilizatori ai sistemului, dosarelor personale ale copiilor, elevilor, studenților, angajaților;
- 2) organele locale de specialitate în domeniul învățământului sunt gestionate în SIME de către deținătorul sistemului;
- 3) instituțiile de învățământ sunt gestionate în SIME de către deținătorul sistemului;
- 4) subdiviziunile structurale sunt gestionate în SIME de către instituțiile de învățământ;
- 5) copiii, elevii, studenții, angajații sunt gestionați în SIME de către instituțiile de învățământ;
- 6) utilizatorii de nivel național și utilizatorii de nivel local sunt gestionați în SIME de către deținătorul sistemului;
- 7) în cazul instituțiilor de învățământ de subordonare locală, utilizatorii de nivel instituțional sunt gestionați în SIME de către organul local de specialitate în domeniul învățământului, iar în cazul instituțiilor de subordonare centrală – de către deținătorul sistemului;
- 8) utilizatorii la nivel de subdiviziuni structurale sunt gestionați în SIME de către instituțiile de învățământ.
- 9) actele de studii ale absolvenților sunt introduse în SIME de către operatorul subdiviziunii structurale;
- 10) SIME poate conține mecanisme directe sau prin fișiere de import al datelor din alte sisteme informaționale din domeniul educațional la nivel național.
- 11) *Transferul copiilor, elevilor, studenților, dintr-o subdiviziune structurală în alta.* În cadrul uneia și aceiași instituție de învățământ transferul se efectuează de către instituția de învățământ.
- 12) *Transferul copiilor, elevilor, studenților dintr-o instituție de învățământ în alta.* Transferul presupune efectuarea a două operații: (1) prima instituție de învățământ declară persoana plecată ca fiind exmatriculată și (2) instituția a doua de învățământ importă persoana venită ca fiind înmatriculată.

13) *Transferul angajaților dintr-o instituție în alta.* Transferul presupune efectuarea a două operații: (1) prima instituție de învățământ declară persoana plecată ca fiind concediată și (2) instituția a doua de învățământ importă persoana venită ca fiind angajată.

14) *Scoaterea obiectului informațional din evidență* se realizează prin radierea acestuia din sistem. Obiectul radiat nu va fi eliminat fizic din baza de date. Radierea constă în schimbarea statului obiectului și al informațiilor asociate acestuia, astfel încât obiectul informațional radiat va figura în sistem doar în calitate de istoric.

### **Secțiunea 3. Interacțiunea cu clasificatoarele, alte sisteme și platforme electronice guvernamentale**

30. În scopul asigurării veridicității, excluderii inconsistenței datelor și micșorării volumului informației păstrate în SIME, în sistem vor fi utilizate următoarele clasificatoare:

1) *Clasificatoare naționale:*

- a) Clasificatorul programelor educaționale din Republica Moldova (MoldCED); Plan cadru
- b) Clasificatorul unităților administrativ/teritoriale (CUATM);
- c) Clasificatorul formelor de proprietate (CFP);
- d) Clasificatorul ocupațiilor din Republica Moldova (CORM 006-14);
- e) Clasificatorul activităților economice (CAEM);
- f) Clasificatorul formelor organizațional-juridice ale agenților economici.

2) *Clasificatoare interne:*

- a) Clasificatorul tipurilor de instituții de învățământ;
- b) Clasificatorul posturilor didactice, de conducere, didactice auxiliare, științifice, științifico-didactice, nedidactice, auxiliare din învățământ;
- c) Clasificatorul tipurilor de planuri-cadru;
- d) Clasificatorul tipurilor de planuri de studii;
- e) Clasificatorul tipurilor de situațiilor de risc în care se pot afla copiii, elevii, studenții;
- f) Clasificatorul tipurilor de vulnerabilitate care pot afecta copiii, elevii, studenții;
- g) Elaborarea clasificatoarelor interne se va face în baza definițiilor de metadate, utilizate în sistemul național de statistică.

31. În scopul funcționării eficiente și asigurării consistenței datelor, SIME va fi integrat cu următoarele sisteme informat:

1) Sistemul informațional automatizat “Registrul de stat al populației”, care include date despre persoanele fizice – în vederea preluării și validării înregistrărilor, modificărilor sau radierilor datelor despre persoanele fizice și a verificării acestora privind combinațiile de IDNP, nume, prenume, gen și data nașterii.

2) Sistemul informațional automatizat “Registrul de stat al unităților de drept”, care conține informații despre toate categoriile de unități de drept, constituite în bază legală – în scopul preluării și validării datelor despre persoanele juridice privind corectitudinea combinațiilor de IDNO, denumire, cod CUATM, cod CAEM etc., necesară înregistrărilor, modificărilor sau radierilor datelor despre persoanele juridice.

3) Sistemul informațional automatizat “Registrul unic de licențiere” – pentru obținerea informației privind instituțiile și organizațiile ce activează în domeniul învățământului.

4) Sistemul informațional automatizat al Biroului Național de Statistică – în scopul prelucrării datelor despre unitățile statistice din domeniul educației.

5) Alte sisteme informaționale /registre naționale care conțin date relevante.

32. SIME va fi interconectabilă și integrată cu platforma de interoperabilitate (MConnect), prin intermediul căreia se va asigura schimbul de date între acesta și alte sisteme și resurse informaționale de stat, în conformitate cu cadrul normativ în domeniul schimbului de date și interoperabilității.”

## **Capitolul VII SPAȚIUL TEHNOLOGIC AL SIME**

33. SIME va fi dezvoltat urmărind o arhitectură în multi-nivel (având cel puțin următoarele nivele - baza de date, logica de aplicație și interfața cu utilizatorul). Utilizarea unei arhitecturi modulare permite o cuplare redusă între componente, în care responsabilitățile fiecărei componente sunt specializate, permite adăugarea de noi module fără modificări în modulele software finalizate.

34. Platforma tehnică va utiliza standarde deschise și va fi compatibilă cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

35. SIME va fi găzduită pe platforma tehnologică guvernamentală comună MCloud, care permite accesul, la cerere, pe bază de rețea la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu rețele, servere, echipamente de stocare, aplicații și servicii) și care pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SIME va putea fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

36. Mijloacele de asigurare a interoperabilității SIME vor corespunde cerințelor stabilite prin actele legislative și normative în vigoare.

37. Mijloacele hardware și software vor garanta stabilirea nivelurilor de acces la sistem în funcție de domeniile de responsabilitate ale fiecărui din utilizatori.

38. Infrastructura informațională a SIME se va baza pe o arhitectură în trei niveluri, caracterizată prin următoarele elemente de bază:

1) *Nivelul de stocare a datelor* – destinat pentru stocarea și actualizarea datelor despre copii, elevi, studenți, angajați, instituțiile de învățământ, organele locale de specialitate în domeniul învățământului, acte de studii și calificări, utilizatori ai sistemului.

2) *Nivelul aplicațiilor* – destinat pentru executarea proceselor de business-logică a SIME.

3) *Nivelul de interacțiune* – reprezintă interfețe destinate utilizatorilor sistemului.

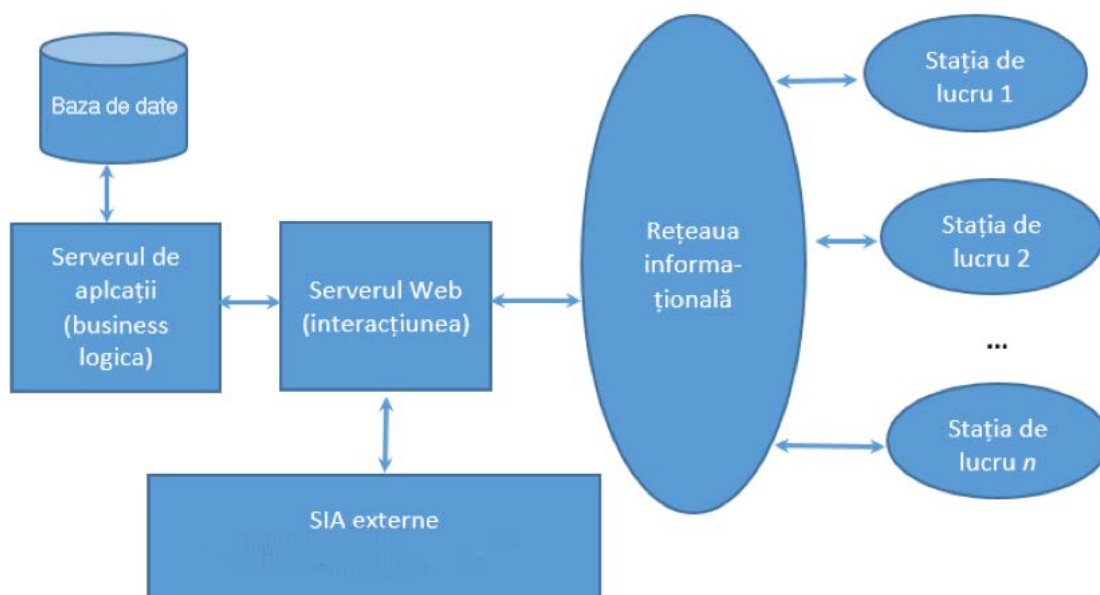


fig. 1 Arhitectura SIME

39. Rețeaua informațională de telecomunicații va asigura accesul la resursele informaționale ale SIME prin protocoale securizate de Internet. Conexiunile securizate de Internet vor fi oferite de către prestatorii naționali de astfel de servicii. Capacitatea serviciilor de comunicare va fi suficientă pentru a asigura buna funcționare a sistemului, oferind posibilitatea ca gestiunea și funcționalitatea fluxurilor de lucru, a documentelor și înregistrărilor să se efectueze online, prin intermediul serviciilor securizate Web.

40. Arhitectura produselor software ale nivelului de stocare a datelor, nivelului aplicațiilor și nivelului de interacțiune va fi una modulară, fapt ce va permite proiectarea și elaborarea eșalonată a componentelor SIME. Lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale va fi stabilită de către elaboratorul sistemului în așa mod încât să se asigure implementarea autonomă și în volum deplin a fiecăruia din contururile funcționale ale SIME.

41. Produsele software ale serverului de aplicații și ale serverului Web vor fi proiectate și elaborate în așa mod, încât accesul la SIME de la stațiile de lucru ale utilizatorilor să poată fi asigurat cu ajutorul produselor program cu destinație generală – programe de navigare în Internet, procesoare de texte, procesoare de calcul tabelar, programe și dispozitive de autentificare a utilizatorilor etc., fără a fi necesară instalarea unor softuri specializate.

42. Având în vedere importanța SIME în cadrul resurselor informaționale de stat ale Republicii Moldova, este necesară o disponibilitate înaltă și accesul neîntrerupt la sistem. Din acest motiv, întreaga soluție va fi construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână).

## **Capitolul VIII**

### **ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SIME**

43. Pentru asigurarea îndeplinirii cerințelor de securitate, vor fi respectate următoarele principii de bază:

1) confidențialitate - asigurarea protecției resurselor de date educaționale împotriva acceselor neautorizate. Accesul la date este limitat doar la participanții autorizați;

2) integritate - asigurarea completitudinii resurselor de date educaționale, dar și asigurarea împotriva manipulării frauduloase a datelor. Protecția împotriva dezastrelor va fi realizată prin crearea copiilor de rezervă incrementale și depline;

3) disponibilitate - sistemul va asigura un proces de redundanță pentru a asigura participanții de eventualele defecțiuni care pot surveni în timpul funcționării precum și asigurarea datelor, componentelor funcționale și serviciilor asociate către utilizatorii autorizați la momentul solicitării;

4) autenticitate - garantarea faptului că datele nu au fost modificate. Pe lângă autenticitate, este important să se asigure și non-repudierea datelor, adică autorii nu vor putea nega proveniența acestora.

44. Utilizatorii vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia.

45. Esența securității informaționale a SIME constă în următoarele:

1) Prin securitate informațională se înțelege protecția resurselor și a structurii informaționale a SIME împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanților la procesele de colectare, stocare, prelucrare și schimb de informații.

2) Noțiunea de securitate informațională a SIME include o serie de termeni cum ar fi: măsuri, politici, tehnologii, puncte de control, structură organizațională, atribuții și funcții în sistem. În procesul elaborării și exploatării SIME se va asigura identificarea și implementarea mijloacelor ce vor asigura securitatea informațională a SIME.

3) Colectarea, prelucrarea, stocarea, transmiterea și furnizarea datelor cu caracter personal se va efectua în conformitate cu prevederile actelor normative și legislative în vigoare.

4) Pentru a asigura nivelul securității informaționale stabilit de actele normativ-legislative în vigoare, la elaborarea și implementarea măsurilor de securitate se va ține cont de cele două aspecte ale acestora – securitatea fizică și securitatea informației:

a) securitatea fizică se referă la protejarea infrastructurii fizice a deținătorului și a registratorilor sistemului, a componentelor fizice (punctele de acces în incinta sălilor cu echipamentele digitale, accesul la calculatoare, imprimante, echipamente de rețea) prin aplicarea tuturor măsurilor de securitate. Securitatea fizică a serverului SIME este asigurată de către deținătorul platformei tehnologice guvernamentale MCloud;

b) securitatea informației se referă la protejarea datelor prin aplicarea unor măsuri de securizare la nivel logic, prin utilizarea tehnologiilor informației. Aceasta include programele antivirus, programe de tip „firewall”, programe de criptare a fișierelor și purtătorilor externi de informație, delimitarea logică a subrețelelor.

46. La elaborarea și exploatarea SIME se va ține cont de actele normative în vigoare cu privire la securitatea cibernetică.

47. În scopul asigurării securității informaționale, la elaborarea și exploatarea SIME vor fi respectate și îndeplinite cerințele și sarcinile ce urmează:

1) securitatea informațională trebuie să se conformeze cerințelor legislației Republicii Moldova în vigoare, precum și standardelor internaționale care nu contravin legislației naționale și contribui la sporirea gradului de securitate.

2) confidențialitatea informației, care presupune limitarea accesului la anumite categorii de date al persoanelor fără drepturile și împuternicirile corespunzătoare;

3) consistența și integritatea logică a informației, adică prevenirea introducerii, modificării, copierii, actualizării și nimicirii neautorizate a datelor;

4) protecția infrastructurii informaționale împotriva deteriorării și încercării de modificare a funcționării SIME.

## **Capitolul IX ÎNCHEIERE**

48. Implementării SIME poate influența eficientizarea proceselor de management educațional la toate nivelele de învățământ. Datele deschise, furnizate de SIME, vor oferi posibilitatea instituțiilor de învățământ și organelor de conducere a învățământului să extindă participarea reprezentanților societății civile, părinților, tuturor cetățenilor țării în planificarea și desfășurarea procesului educațional, vor crea posibilități de evaluare a instituțiilor de învățământ și a întregului domeniu al educației.

49. Elaborarea și implementarea SIME presupune atât modernizarea software-lor utilizate deja în managementul educațional la nivel central și instituțional, cât și elaborarea de produse-program noi, orientate spre integrarea lor în resursele informaționale de stat. Funcționarea eficientă a SIME va fi condiționată de edificarea integrală a infrastructurii corespunzătoare. Organizarea SIME pe baza principiilor modularității și scalabilității va permite implementarea acestuia pe etape, cu extinderea treptată pe toate nivelurile și ciclurile învățământului din Republica Moldova, în funcție de mijloacele financiare disponibile.

50. Prezentul Concept va servi drept bază pentru elaborarea sarcinilor tehnice destinate proiectării, dezvoltării și introducerii consecutive în exploatare a componentelor ce vor realiza evidența entităților educaționale și vor asigura suportul informațional pentru managementul, monitorizarea și evaluarea fiecărui nivel și ciclu al sistemului de învățământ, a instituțiilor de învățământ de orice tip. Baza de date a SIME va servi în calitate de resursă informațională consolidată pentru dezvoltarea și implementarea pe scară largă a serviciilor educaționale digitale.

51. MECC a Republicii Moldova în comun cu CTICE va evalua anual costurile necesare administrării, funcționării și dezvoltării continue a SIME și va înainta propuneri de solicitare a mijloacelor financiare pentru a fi incluse în proiectul legii bugetului de stat pe anul respectiv.

52. Implementarea efectivă a SIME revine MECC a Republicii Moldova și CTICE în comun cu autoritățile publice locale și instituțiilor de învățământ. La îndeplinirea obiectivelor prezentei Concepții pot participa și alte instituții ale statului, precum și organizații neguvernamentale, care cooperează potrivit competențelor și în condițiile legii.

## **REGULAMENTUL** **privind utilizarea și administrarea Modulului Educație Timpurie al SIME**

### **Capitolul I** **DISPOZIȚII GENERALE**

#### **Obiectul de reglementare**

1. Modulul Educație timpurie al Sistemului Informațional de Management în Educație (SIME), în continuare Modul, include totalitatea informației cu caracter educațional referitoare la educația timpurie.

2. Regulamentul privind Modulul, în continuare Regulament, stabilește procedurile și mecanismele de introducere, stocare, prelucrare și de extragere a datelor referitoare la instituțiile, copii, cadrele didactice, cadrele de conducere și cadrele auxiliare din învățământul educația timpurie.

3. În sensul prezentului Regulament sunt utilizate următoarele noțiuni:

*administrator național* – subdiviziunea responsabilă de gestionarea și operarea resurselor informaționale ale Modulului;

*integritate* – certitudinea, necontradictorialitatea și actualitatea informației, protecția ei de distrugere și modificare neautorizată;

*utilizator* – posesorul și deținătorul, administratorul tehnic, furnizorii și utilizatorii resurselor de instruire, inclusiv, după caz, persoanele fizice și juridice de drept privat care folosesc sistemul pentru introducere, actualizarea datelor educaționale;

*rol* – set de atribuții și sarcini specifice care îi revin participantului la modul după înregistrarea acestuia.

4. Modulul constituie o sursă oficială de informații cu caracter educațional pentru participanții la Modul și pentru toate sistemele informaționale ale autorităților administrației publice centrale și locale care utilizează și prelucrează astfel de tipuri de date. Datele Modulului se consideră corecte și veridice până la proba contrarie.

5. Modulul este un subsistem al SIME.

6. Modulul este elaborat în conformitate cu Conceptul SIME.

### **Capitolul II** **SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ȘI** **FUNCȚIONĂRII MODULULUI**

7. Persoanele fizice, desemnate în calitate de utilizatori ai Modulului, pot avea următoarele roluri:

1) administrator național – are acces la toate informațiile din sistem;

2) administrator raional/municipal – are acces doar la datele referitoare la învățământul din unitatea teritorial-administrativă de care este responsabil;

3) administrator al instituției – are acces doar la datele referitoare la instituția de învățământ în care activează;

4) operator al subdiviziunii structurale – are acces doar la datele referitoare la subdiviziunea de care este responsabil (clasa, grupa etc.);

5) expert - operator al subdiviziunii structurale care are acces doar la datele referitoare la subdiviziunea de care este responsabil (clasa, grupa etc.) cu restricționarea de a modifica datele educaționale;

6) economist- are drepturile similare ca operatorul al subdiviziunii structurale cu accesul la datele economico-financiare;

7) analist raional/național/ instituție - are acces doar la vizualizarea datelor prin rapoartele accesibile;

8. Registratorii Modulului asigură la nivel de stat evidența unică, după cum urmează:

- 1) instituțiile de învățământ – înregistrează, actualizează, radiază datele despre instituții, grupe, copii, angajați, utilizatori ai sistemului din cadrul instituțiilor de învățământ în cauză;
- 2) organele locale de specialitate în domeniul învățământului – înregistrează, actualizează, radiază datele despre organele de specialitate, rețeaua de instituții de învățământ din unitățile teritorial-administrative în cauză, angajații și utilizatorii sistemului din cadrul organelor de specialitate în cauză;
- 3) deținătorul Modulului – înregistrează, actualizează, radiază datele despre rețeaua de instituții de învățământ aflate în subordinea MECC, altor organe ale administrației publice centrale, utilizatorii sistemului din cadrul administrației publice centrale.

9. Obiectele înregistrării conținute în Modul sunt:

- 1) instituția de învățământ;
- 2) copilul;
- 3) personalul didactic;
- 4) personalul de conducere;
- 5) personalul auxiliar;
- 6) Utilizatorii Modulului.

### **Capitolul III** **DREPTURILE, ATRIBUȚIILE ȘI OBLIGAȚIILE** **PARTICIPANȚILOR LA MODUL**

#### **Secțiunea 1**

#### **Drepturile, atribuțiile și obligațiile deținătorului Modulului**

10. Deținătorul are următoarele drepturi:

- 1) să elaboreze și să dezvolte, prin intermediul Cancelariei de Stat, în baza competențelor sale, cadrul normativ cu privire la Modul;
- 2) să propună soluții de perfecționare și eficientizare a procesului de funcționare a Modulului, precum și să le pună în aplicare;
- 3) să supravegheze respectarea cerințelor de securitate a informației de către participanții la Modul, să fixeze cazurile și tentativele de încălcare a acestora;
- 4) să inițieze procedura de revocare a accesului la Modul pentru utilizatorii care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale;
- 5) să verifice autenticitatea și veridicitatea datelor educaționale introduse de participanții la Modul;
- 6) să solicite de la participanți actualizarea sau corectarea datelor Modulului, în caz de depistare a omiterilor și erorilor.

11. Deținătorul are următoarele atribuții:

- 1) asigură condițiile organizatorice și financiare pentru funcționarea Modulului;
- 2) stabilește scopurile și funcționalitățile Modulului;
- 3) determină obiectele informaționale supuse înregistrării în Modul și conținutul acestora;
- 4) asigură securitatea și protecția datelor din Modul;
- 5) aprobă și coordonează cu administratorul tehnic executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale Modulului, erorile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea normală al acestuia;
- 6) asigură dezvoltarea continuă a Modulului prin adăugarea de noi componente ce pot fi utilizate de participanți în cadrul Modulului;
- 7) autorizează, suspendă și revocă dreptul de acces în Modul;
- 8) stabilește măsurile tehnice și organizatorice de protecție și securitate a Modulului;
- 9) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a Modulului la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;
- 10) organizează seminare și instruirii de promovare și utilizare a Modulului pentru furnizori și resurse de instruire;

11) asigură acordarea suportului metodologic și tehnic participanților la Modul în procesul de gestionare a resurselor de date educaționale pe modul, inclusiv prin elaborarea și menținerea ghidului metodologic privind introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor educaționale, precum și funcționarea Modulului;

12) monitorizează și supraveghează accesările informației din Modul și identifică încălcările comise;

13) exercită alte atribuții necesare asigurării bunei funcționări a Modulului.

12. Deținătorul are următoarele obligații:

1) să asigure funcționarea neîntreruptă și ținerea Modulului în conformitate cu cadrul normativ în vigoare;

2) să acorde suportul necesar persoanelor autorizate, care au acces la Modul, privind utilizarea complexului de mijloace software aferente acestuia;

3) să informeze participanții la Modul despre modificările condițiilor tehnice de funcționare a acestuia;

4) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a informației și a datelor cu caracter personal;

5) să utilizeze informația obținută din Modul doar în scopurile stabilite de prezentul regulament și cadrul normativ în vigoare.

## **Secțiunea a 2-a**

### **Drepturile, atribuțiile și obligațiile Administratorului Național IET al Modulului**

13. Administratorul Național are dreptul:

1) să supravegheze respectarea cerințelor de securitate informațională și cibernetică de către utilizatori, să fixeze cazurile și tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea și lichidarea consecințelor, precum și să informeze posesorul SIME;

2) să solicite de la utilizatori colectarea și actualizarea informațiilor în Modul;

3) să inițieze procedura de suspendare și revocare a drepturilor de acces la Modul în cazurile de nerespectare a prezentului regulament și a actelor normative cu privire la securitatea informațională/cibernetică;

4) să stabilească cerințe față de mijloacele tehnice, canalele telecomunicaționale și software la locurile automatizate de muncă ale utilizatorilor;

5) să propună căi suplimentare de perfecționare și eficientizare a funcționării Modulului.

14. Administratorul Național are următoarele atribuții:

1) să asigure funcționarea și menținerea Modulului în corespundere cu prezentul regulament și actele normative în vigoare;

2) să asigure suportul metodologic și practic pentru toți utilizatorii Modulului cu referire la menținere, actualizarea și utilizarea datelor cu caracter educațional;

3) să asigure colectarea informațiilor, stocarea lor, menținerea și actualizarea Modulului;

4) să verifice, în limita competențelor, veridicitatea informațiilor colectate în Modul;

5) să acorde utilizatorului acces la informația din Modul în conformitate cu prezentul regulament și actele normative în vigoare. În caz de modificare a drepturilor de acces, administratorul trebuie să ia decizia cu privire la reconfigurarea acestora în caz de necesitate;

6) să efectueze, în limitele competențelor, măsurile necesare privind protecția și confidențialitatea informațiilor din Modul, inclusiv împotriva accesului, corectării, modificării și transmiterii neautorizate;

7) să asigure măsurile necesare pentru securitatea cibernetică și a datelor cu caracter personal în corespundere cu actele normative în vigoare;

8) să efectueze monitorizarea activităților utilizatorilor din Modul;

9) să informeze utilizatorii despre modificările organizatorice / tehnice de funcționare a Modulului.

15. Administratorul Național este obligat:

1) să asigure funcționarea și menținerea Modulului în corespundere cu prezentul regulament și actele normative în vigoare;

- 2) să asigure suportul metodologic și practic pentru toți utilizatorii Modulului cu referire la menținerea, actualizarea și utilizarea datelor cu caracter educațional;
- 3) să asigure colectarea informațiilor, stocarea lor, menținerea și actualizarea Modulului;
- 4) să verifice, în limita competențelor, veridicitatea informațiilor colectate în Modul;
- 5) să acorde utilizatorului acces la informația din Modul în conformitate cu prezentul regulament și actele normative în vigoare. În caz de modificare a drepturilor de acces, administratorul trebuie să ia decizia cu privire la reconfigurarea acestora în caz de necesitate;
- 6) să efectueze, în limitele competențelor, măsurile necesare privind protecția și confidențialitatea informațiilor din Modul, inclusiv împotriva accesului, corectării, modificării și transmiterii neautorizate;
- 7) să asigure măsurile necesare pentru securitatea cibernetică și a datelor cu caracter personal în corespundere cu actele normative în vigoare;
- 8) să efectueze monitorizarea activităților utilizatorilor din Modul;
- 9) să informeze utilizatorii despre modificările organizatorice / tehnice de funcționare a Modulului.

### **Secțiunea a 3-a** **Atribuțiile registratorului Modulului**

16. Registratorul Modulului are următoarele atribuții:
- 1) asigură corectitudinea și autenticitatea datelor introduse sau prezentate pentru a fi introduse în Modul;
  - 2) transmite către deținător și actualizează informația prezentată cu privire la utilizatori;
  - 3) asigură confidențialitatea și autenticitatea datelor transmise spre utilizare în cadrul Modulului;
  - 4) raportează deținătorului Modulului problemele de funcționalitate ale acesteia;
  - 5) plasează și deține propriile resurse de date educaționale în Modul;
  - 6) asigură calitatea datelor educaționale în Modul în conformitate cu cadrul normativ de profil;
  - 7) asigură securitatea informațională a datelor educaționale plasate în Modul;
  - 8) utilizează resursele tehnologice comune ale Modulului;
  - 9) oferă sugestii de îmbunătățire și contribuie la dezvoltarea continuă a Modulului prin adăugarea de noi componente ce pot fi reutilizate de alți beneficiari la gestionarea datelor în Modul;
  - 10) alte atribuții aferente furnizării de date în Modul.

### **Secțiunea a 4-a** **Obligațiile și drepturile utilizatorilor Modulului**

17. În funcție de rol, utilizatorii Modulului sunt obligați:
- 1) să asigure înregistrarea, actualizarea, colectarea, prelucrarea și transmiterea informațiilor cu caracter educațional în Modul;
  - 2) să respecte disciplina de înregistrare, evidență și utilizare a informației cu caracter educațional conform actelor normative;
  - 3) să asigure autenticitatea, veridicitatea datelor introduse în Modul și actualizarea acestora;
  - 4) să asigure și să efectueze controlul sistemului de securitate, să înștiințeze despre cazurile și tentativele de încălcare a acestuia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor;
  - 5) să asigure securitatea accesului la informația conținută în Modul, respectarea condițiilor de securitate și regulilor de exploatare a Modulului;
  - 6) să asigure condițiile necesare pentru păstrarea în siguranță a suporturilor materiale, precum și pentru excluderea accesului terțelor persoane la suporturile respective;
  - 7) să asigure implementarea măsurilor de securitate cibernetică în conformitate cu actele normative;

- 8) să utilizeze informația obținută din Modul doar în scopurile stabilite de actele normative cu respectarea legislației privind dreptul de autor și drepturile conexe;
- 9) să înștiințeze neîntârziat, în formă verbală și scrisă, administratorul Modulului despre cazurile de încălcare a securității informaționale în conformitate cu actele normative;
- 10) să aducă la cunoștința deținătorului modului, în termen de o zi, orice situație de imposibilitate fortuită de executare (incidente aflate în afara ariei de competență a utilizatorului) care ar putea influența în mod negativ exercitarea funcțiilor utilizatorilor.
- 11) să aducă la cunoștința celorlalți utilizatori, în termen de o zi, orice situație de forță majoră care ar putea influența în mod negativ funcționarea sistemului;
- 12) să aducă la cunoștința Administratorului ierarhic superior despre încetarea raporturilor de muncă/de serviciu.
- 13) să asigure colectarea, introducerea și prelucrarea informației relevante în Modul, conform ghidului metodologic pus la dispoziția participanților la Modul, precum și în termenele coordonate cu deținătorul acestuia;
- 14) să ia măsurile organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu instrucțiunile deținătorului Modulului.
18. Directorii instituțiilor de educație timpurie sunt obligați:
- 1) să asigure, să organizeze și să amenajeze locuri de muncă în instituție pentru persoanele responsabile de înregistrarea, actualizarea, colectarea și prelucrarea informației cu caracter educațional.
- 2) să asigure deservirea tehnică a componentelor și să înlăture defecțiunile tehnice ale locurilor de muncă automatizate conectate la Sistem.
- 3) să asigure veridicitatea, plenitudinea și actualitatea datelor.
- 4) să prezinte electronic Administratorului raional/municipal SIME Raportul de confirmare a directorului instituției de învățământ, semnat digital, cu privire la veridicitatea, plenitudinea și actualitatea datelor din Modul. Raportul va fi prezentat la sfârșitul fiecărei perioade de actualizare SIME.
19. Fiecare utilizator are următoarele drepturi:
- 1) să participe la implementarea și dezvoltarea Modulului, în limitele drepturilor indicate în prezentul Regulament;
- 2) să înainteze deținătorului Modulului propuneri privind modificarea și/sau completarea actelor normative care reglementează funcționarea Modulului;
- 3) să solicite și să primească de la deținătorul posesorul Modulului ajutor metodologic și practic privind funcționarea acesteia;
- 4) să prezinte propuneri deținătorului Modulului platformei privind perfecționarea și eficientizarea funcționării acesteia.

## **Capitolul IV**

### **GESTIONAREA ȘI ASIGURAREA FUNCȚIONĂRII MODULULUI**

20. Modulul se ține în limba de stat, rusă și engleză.
21. Baza de date a Modulului este parte a bazei de date SIME și asigură evidența centralizată a informației referitoare la instituțiile de învățământ, copii, cadre didactice, nedidactice, conducere și auxiliare, precum și eliberarea rapoartelor statistice generalizate privind starea sistemului de educație timpurie.
22. Introducerea datelor în Modul se efectuează în baza documentelor primare sau din alte sisteme informaționale, care conțin datele necesare.
23. Evidența obiectelor informaționale se ține conform metodologiilor coordonate/ aprobate de către posesorul Sistemului.
24. În cazul depistării unor erori sau inexactități în datele introduse, utilizatorii modulului sunt obligați să informeze despre aceasta administratorul de rang mai înalt, care va asigura eliminarea acestora din modul.
25. Dacă furnizorul datelor Modulului nu are drepturile necesare pentru a corecta erorile în sistem, se va adresa la nivelul superior printr-un demers argumentat privind rectificarea datelor eronate sau inexacte.

26. Radierea datelor din Modul se efectuează de către administratorul Modulului în baza deciziei registratorului, cu respectarea strictă a cerințelor privind protecția datelor cu caracter personal. Radierea datelor se face prin inserarea unei note speciale și nu reprezintă excluderea fizică a datelor din Modul.

27. Funcționarea Modulului este asigurată de deținător până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării Modulului, datele și documentele conținute în acesta se transmit în arhivă conform actelor normative.

28. Datele din Modul ce dezvăluie originea etnică a persoanei, apartenența socială și datele privind starea de sănătate fac parte din categoria specială a datelor cu caracter personal. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul Modulului se efectuează cu respectarea strictă a actelor normative.

29. Accesul la Modul se realizează în regim eficient și neîntrerupt.

30. Perioadele de actualizare a datelor sunt stabilite de MECC prin ordine aprobate.

31. Confirmarea veridicității datelor introduse în sistem, va fi efectuată prin aplicarea semnăturii electronice de către administratorul instituției.

## **Capitolul V**

### **REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN MODUL**

#### **Secțiunea 1**

##### **Acordarea dreptului de acces la Modul**

32. Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea numelui, prenumelui, IDNP-ului, funcției, e-mailului personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

33. Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective. Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces, întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

34. Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.

35. Accesul la datele din Modul se acordă în conformitate cu actele normative privind accesul la informație. Utilizatorii beneficiază de drepturi egale de acces la informația din Modul, în limitele rolurilor atribuite și nu sunt obligați să justifice, în fața posesorului/deținătorului Modulului, necesitatea obținerii informației solicitate, cu excepția datelor cu caracter personal.

36. Accesul la funcționalitățile Modulului sunt condiționate de rolul utilizatorului.

37. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

38. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

39. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

40. Participanții au drept de acces la informația din Modul conform atribuțiilor și funcțiilor deținute și regimului juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și/sau profilului de acces.

41. Informația conținută în Modul se divizează în:

1) informații publice accesibile tuturor utilizatorilor, inclusiv a informației de pe interfața Modulului, care pot fi accesate fără necesitatea autentificării în sistem;

2) informații cu acces limitat, care sunt puse la dispoziția angajaților entităților publice și a utilizatorilor privați care, pentru accesare, necesită autentificare în sistem.

42. La înregistrarea în cadrul Modulului, fiecărui utilizator i se atribuie un identificator unic și rolul de care depinde dreptul de acces la obiectele informaționale. Autorizarea utilizatorilor se

produce în conformitate cu nivelul de acces stabilit și utilizatorii au posibilitatea să acceseze funcționalitățile sau informațiile disponibile potrivit nivelului de acces.

43. La baza mecanismului de autentificare în cadrul Modulului se află serviciul electronic guvernamental de autentificare și control al accesului (MPass). Utilizatorii care nu au semnătură electronică vor putea fi autentificați în Modul în baza de nume și parolă, oferite de către deținător.

44. Dreptul de acces la resursele informaționale ale Modulului este segmentat pe unități de conținut, atribuind prerogative partajate, și anume: vizualizare, adăugare, redactare și ștergere.

45. Accesul la resursele informaționale ale Modulului este segmentat pentru utilizatorii interni și utilizatorii externi.

46. Utilizatori interni ai Modulului sunt deținătorul platformei și administratorul de sistem, ale căror drepturi de acces sunt definite în prezentul Regulament și alte acte normative.

47. Posesorul Modulului are acces cu drept de vizualizare a datelor din Modul, în limita scopului și atribuțiilor acordate prin prezentul Regulament și cadrul normativ în vigoare.

48. Accesul la datele Modulului se realizează prin:

- 1) acordarea accesului public la informația nerestricționată, plasată pe Modul;
- 2) acordarea accesului utilizatorilor externi, în limitele prezentului Regulament;
- 3) acordarea accesului utilizatorilor interni, precum și registratorilor din cadrul entităților juridice, în limitele competențelor.

49. La acordarea accesului utilizatorilor la datele educaționale, utilizatorul acestora asigură respectarea legislației privind dreptul de autor și drepturile conexe.

50. Exploatarea Modulului fără autorizare nominală este strict interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public, cu excepția exploatării resurselor de instruire publice plasate în Modul.

51. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

52. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

53. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

## **Secțiunea a 2-a**

### **Revocarea dreptului de acces la Modul**

54. Dreptul de acces la Modul nu este unul permanent și poate fi revocat în circumstanțele prevăzute de prezentul Regulament. Introducerea și/sau modificarea datelor din Modul de pe un nume sau profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Participanții la Modul urmează să se asigure că profilul de utilizator, precum și semnătura electronică sunt confidențiale.

55. Revocarea dreptului de acces la Modul pentru utilizatori se efectuează în una dintre următoarele situații:

- 1) în temeiul notificării conducătorului acestuia;
- 2) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;
- 3) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele din Modul;
- 4) la constatarea încălcării de către utilizator a prezentului regulament.

56. Revocarea dreptului de acces la Modul se efectuează de deținător, în una din următoarele situații:

- 1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale registratorului/utilizatorului Modulului;
- 2) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților registratorului/utilizatorului, când noile atribuții nu impun accesul la datele Modulului;
- 3) la suspendarea/expirarea/rezilierea sau revocarea contractului de prestări servicii educaționale încheiat între deținătorul și utilizatorul datelor educaționale;
- 4) în alte cazuri, în limitele legislației.

57. Revocarea dreptului de acces la Modul se poate efectua de către deținătorul platformei, în una din următoarele situații:

- 1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale angajaților deținătorului Modulului;
- 2) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților deținătorului Modulului, când noile atribuții nu impun accesul la datele Modulului;
- 3) la încălcarea regulilor de utilizare a sistemului sau la constatarea încălcării securității informaționale de către utilizatori;
- 4) la cererea expresă a participanților la Modul, pentru sine sau utilizatorii săi de date educaționale;
- 5) în alte cazuri, în limitele legislației.

58. Accesul la datele din Modul se acordă în conformitate cu actele normative privind accesul la informație. Utilizatorii beneficiază de drepturi egale de acces la informația din Modul, în limitele rolurilor atribuite și nu sunt obligați să justifice, în fața posesorului/deținătorului Modulului, necesitatea obținerii informației solicitate, cu excepția datelor cu caracter personal.

59. Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea numelui, prenumelui, IDNP-ului, funcției, e-mailul personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

60. Revocarea dreptului de acces la Modul pentru utilizatori se efectuează în una dintre următoarele situații:

- 1) în temeiul notificării conducătorului acestuia;
- 2) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;
- 3) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele din Modul;
- 4) la constatarea încălcării de către utilizator a prezentului regulament.

61. Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective.

62. Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

63. Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.

64. Accesul la funcționalitățile Modulului este condiționat de rolul utilizatorului.

65. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

66. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

67. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

## **Capitolul VI**

### **INTERACȚIUNEA CU ALTE SERVICII ȘI PLATFORME ELECTRONICE GUVERNAMENTALE**

68. Modulul este găzduit pe platforma tehnologică guvernamentală comună (MCloud), care permite accesul, la cerere, pe bază de rețea, la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu: rețele, servere echipamente de stocare, aplicații și servicii) ce pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SIME poate fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

69. Modulul utilizează următoarele servicii electronice și platforme guvernamentale:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 1090/2013 „Privind serviciul electronic guvernamental de autentificare și control al accesului (MPass)”;

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 405/2014 „Privind serviciul electronic guvernamental integrat de semnătură electronică (MSign)”;

3) serviciul electronic guvernamental de jurnalizare (MLog) – instrument securizat și flexibil de jurnalizare și audit, utilizat pentru asigurarea evidenței operațiunilor (evenimentelor) produse în SIME și registrele formate de acesta.

## **Capitolul VII**

### **ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI MODULULUI**

#### **Secțiunea 1**

##### **Securitatea informației în Modul**

70. Serviciile furnizate de Modul se conformează cerințelor minime de securitate corespunzătoare cerințelor de securitate a aplicațiilor livrate din platforma MCloud.

71. Măsurile de protecție și securitate a informației cu caracter educațional din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIME și se efectuează neîntrerupt de către toți utilizatorii.

72. Protecția informației din Modul se efectuează prin următoarele metode:

1) folosirea metodelor de cifrare și criptare a informațiilor din Modul;

2) prevenirea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor sau defecțiuni în funcționarea complexului tehnic și de program, asigurată prin metoda folosirii mijloacelor de protecție speciale de program, antivirus și efectuarea periodică a copiilor de rezervă.

73. Fiecare instituție elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională și cibernetică pentru asigurarea respectării prezentului regulament și a actelor normative în vigoare.

74. Fiecare instituție desemnează o persoană responsabilă de actualizarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională și cibernetică.

75. Administratorii și operatorii subdiviziunilor structurale pot efectua acțiuni de introducere, modificare, păstrare și extragere a informațiilor cu caracter educațional care se referă doar la unitatea administrativ-teritorială, instituția sau clasa de care sunt responsabili.

76. Analistii nu au acces la datele cu caracter personal și pot efectua doar acțiuni de vizualizare și extragere a informațiilor statistice, referitoare la unitatea administrativ-teritorială sau instituția de care sunt responsabili.

77. Măsurile de protecție și securitate a informației cu caracter personal din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a Modulului și se efectuează neîntrerupt de către toți participanții.

78. Obiecte ale asigurării protecției și securității informației din Modul se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

1) platforma guvernamentală, sistemele operaționale, sistemele de gestiune a Modulului, sistemele de evidență și alte aplicații care asigură funcționarea Modulului;

2) sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

79. Protecția informației cu caracter personal în Modul la nivel de deținător ale acesteia se efectuează prin următoarele metode:

1) asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport date;

2) excluderea accesului neautorizat la datele din Modul prin utilizarea funcționalităților de autorizare ale serviciului MPass;

3) prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau cauzează defecțiuni în funcționarea complexului tehnic și de program;

4) efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;

5) efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării Registrului în cazul incidentelor.

80. Protecția informației cu caracter personal la nivel de participant la Modul se efectuează prin următoarele metode:

1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor din Modul;

2) monitorizarea procesului de exploatare a Modulului prin intermediul mecanismului de jurnalizare efectuat de deținătorul acestuia.

81. Participanții la Modul elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, incluzând:

1) identitatea persoanei responsabile de politica de securitate;

2) principalele măsuri tehnico-organizatorice necesare asigurării funcționării Modulului;

3) procedurile interne ce exclud cazurile de modificare nesanționată a mijloacelor software și/sau a informației din Modul;

4) responsabilitățile personalului participantului la Modul privind asigurarea securității informaționale;

5) procedurile de control intern al participantului la Modul privind respectarea condițiilor de securitate informațională.

82. Fiecare participant la Modul asigură informarea sau, după caz, instruirea utilizatorilor privind metodele și procedeele de contracarare a pericolelor informaționale.

## **Secțiunea a 2-a**

### **Protecția datelor cu caracter personal din Modul**

83. Datele de autentificare în Modul fac parte din categoria datelor cu caracter personal. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul Modulului se efectuează de către subiecții cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

84. Măsurile de protecție și securitate a informației cu caracter educațional din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIME și se efectuează neîntrerupt de către toți utilizatorii.

85. Protecția informației din Modul se efectuează prin următoarele metode:

1) folosirea metodelor de cifrare și criptare a informațiilor din Modul;

2) prevenirea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor sau defecțiuni în funcționarea complexului tehnic și de program, asigurată prin metoda folosirii mijloacelor de protecție speciale de program, antivirus și efectuarea periodică a copiilor de rezervă.

86. Fiecare instituție elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională și cibernetică pentru asigurarea respectării prezentului regulament și a actelor normative în vigoare.

87. Fiecare instituție desemnează o persoană responsabilă de actualizarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională și cibernetică.

88. Administratorii și operatorii subdiviziunilor structurale pot efectua acțiuni de introducere, modificare, păstrare și extragere a informațiilor cu caracter educațional care se referă doar la unitatea administrativ-teritorială, instituția sau clasa de care sunt responsabili.

89. Analistii nu au acces la datele cu caracter personal și pot efectua doar acțiuni de vizualizare și extragere a informațiilor statistice, referitoare la unitatea administrativ-teritorială sau instituția de care sunt responsabili.

## **Capitolul VIII**

### **SUSPENDAREA FUNCȚIONĂRII MODULULUI**

90. Pentru asigurarea funcționalității eficiente și neîntrerupte, schimbul informațional de date în Modul este asigurat în regim non-stop.

91. Funcționarea Modulului se suspendă de către administratorul tehnic, după coordonarea prealabilă cu deținătorul Modulului, în cazul apariției uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al Modulului;

2) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea Modulului;

3) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al Modulului;

4) la cererea scrisă a posesorului Modulului.

92. Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea, în scris sau prin e-mail, a furnizorilor de resurse de instruire de către deținătorul Modulului, în baza planului coordonat cu administratorul tehnic, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea furnizorilor de resurse de instruire și coordonarea prealabilă cu deținătorul Modulului, în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware. Dacă lucrările profilactice durează mai mult de 5 de zile, la expirarea fiecărei perioade de 5 de zile de efectuare a lucrărilor, se notifică Furnizorii.

93. Furnizarea serviciilor oferite de Modul poate fi suspendată de către administratorul tehnic fără consimțământul deținătorul Modulului, cu notificarea ulterioară a acestuia, în următoarele situații:

1) situații de incidente la scară;

2) la apariția situațiilor de imposibilitate fortuită de executare;

3) situații de criză.

94. Suspendarea serviciilor se efectuează asigurându-se un impact minim asupra calității serviciilor livrate furnizorilor de resurse de instruire și utilizatorilor acestora.

## **Capitolul IX MONITORIZARE ȘI CONTROL**

### **Secțiunea 1 Controlul extern**

95. Menținerea Modulului este supusă controlului intern, extern și sub aspectul legalității operațiunilor de prelucrare a datelor cu caracter personal. Controlul extern asupra respectării cerințelor privind crearea, menținerea, exploatarea și reorganizarea Modulului poate fi efectuată de către autoritățile împuternicite.

96. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal în cadrul Modulului se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter personal al Republicii Moldova.

97. La efectuarea controlului extern, organul de control alcătuiește un raport privind controlul extern. Deținătorul Modulului este obligat să ia măsuri pentru lichidarea încălcărilor identificate și să informeze despre aceasta organul de control.

98. Pentru organizarea controlului de funcționare a Modulului este responsabil deținătorul Modulului/administratorul tehnic, care este obligat să asigure dreptul de acces la Modul și mijloacele de ținere a acestuia, respectiv în încăperile în care se află mijloacele hardware utilizate în acest scop.

99. Participanții responsabili de asigurarea funcționării Modulului și înregistrării datelor poartă răspundere personală, în conformitate cu cadrul normativ, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.

100. Toți participanții la Modul și destinatarii informațiilor ce conțin date cu caracter personal poartă răspundere conform legislației în vigoare pentru divulgarea, transmiterea acestora persoanelor terțe și pentru utilizarea lor în scopuri personale.

101.Funcționarea Modulului este asigurată de deținătorul Modulului până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

## **Secțiunea a 2-a**

### **Monitorizarea și controlul intern**

102.Controlul intern privind organizarea și funcționarea Modulului se efectuează de către posesorul SIME.

103.Responsabilitatea pentru organizarea și funcționarea Modulului se atribuie administratorului acestuia, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea Modulului. Actele elaborate se coordonează cu posesorul SIME.

104.Persoanele cu funcții de răspundere, în obligațiile cărora intră menținerea Modulului, furnizarea informațiilor din Modul, precum și asigurarea funcționării Modulului, poartă răspundere personală pentru plenitudinea, autenticitatea, veridicitatea, integritatea informațiilor, precum și pentru păstrarea și utilizarea lor. În caz de încălcare, aceștia pot fi trași, potrivit legii, la răspundere disciplinară, civilă, contravențională și/sau penală.

105.În scopul monitorizării și controlului asupra executării Regulamentului, cooperarea dintre posesorul platformei și furnizorul de resurse de instruire va fi asigurată prin schimb de informație, raportare periodică, ședințe comune de evaluare, replanificare, audit etc.

106.Concluziile generate de eforturile de monitorizare, control și evaluare sistematică vor servi drept bază în luarea deciziilor corective pe parcursul implementării platformei, planificarea activităților la diferite etape de operare a platformei, evaluarea performanței participanților la utilizarea platformei, supravegherea procesului de implementare și operare a resurselor informaționale elaborate pe baza platformei etc.

107.Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea numelui, prenumelui, IDNP-ului, funcției, email-ul personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

108.Revocarea dreptului de acces la Modul pentru utilizatori se efectuează în una dintre următoarele situații:

- 5) în temeiul notificării conducătorului acestuia;
- 6) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;
- 7) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele din Modul;
- 8) la constatarea încălcării de către utilizator a prezentului regulament.

109.Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective.

110.Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

111.Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.

# **REGULAMENTUL** **privind utilizarea și administrarea Modulului Învățământ primar, gimnazial și liceal al SIME**

## **Capitolul I** **DISPOZIȚII GENERALE**

### **Obiectul de reglementare**

1. Modulul Învățământ primar, gimnazial și liceal al Sistemului Informațional de Management în Educație (SIME), în continuare Modul include totalitatea informației cu caracter educațional, referitoare la învățământul primar, gimnazial și liceal.

2. Regulamentul privind Modulul, în continuare Regulament stabilește procedurile și mecanismele de introducere, stocare, prelucrare și de extragere a datelor referitoare la instituțiile, elevii, cadrele didactice, nedidactice, conducere și auxiliare din învățământul primar, gimnazial și liceal.

3. În sensul prezentului Regulament sunt utilizate următoarele noțiuni:

*administrator național* – subdiviziunea responsabilă de gestionarea și operarea resurselor informaționale ale Modulului;

*integritate* – certitudinea, necontradictorialitatea și actualitatea informației, protecția ei de distrugere și modificare neautorizată;

*utilizator* – posesorul și deținătorul, administratorul tehnic, furnizorii și utilizatorii resurselor de instruire, inclusiv, după caz, persoanele fizice și juridice de drept privat care folosesc sistemul pentru introducere, actualizarea datelor educaționale;

*rol* – set de atribuții și sarcini specifice care îi revin participantului la modul după înregistrarea acestuia.

4. Modulul constituie o sursă oficială de informații cu caracter educațional pentru utilizatorii Modulului și pentru toate sistemele informaționale ale autorităților administrației publice centrale și locale care utilizează și prelucrează astfel de tipuri de date. Datele Modulului se consideră corecte și veridice până la proba contrarie.

5. Modulul este un subsistem al SIME.

6. Modulul este elaborat în conformitate cu Conceptul SIME.

## **Capitolul II** **SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ȘI FUNCȚIONĂRII** **MODULULUI**

7. Persoanele fizice, desemnate în calitate de utilizatori ai Modulului, pot avea următoarele roluri:

1) administrator național – are acces la toate informațiile din sistem;

2) administrator raional/municipal – are acces doar la datele referitoare la învățământul din unitatea teritorial-administrativă de care este responsabil;

3) administrator al instituției – are acces doar la datele referitoare la instituția de învățământ în care activează;

4) expert - operator al subdiviziunii structurale care are acces doar la datele referitoare la subdiviziunea de care este responsabil (clasa, grupa etc.) cu restricționarea de a modifica datele educaționale;

5) economist- are drepturile similare ca operatorul al subdiviziunii structurale cu accesul la datele economico-financiare;

6) analist raional/național/ instituție - are acces doar la vizualizarea datelor prin rapoartele accesibile;

7) angajat al instituției de formare continuă.

8. Registratorii Modulului asigură la nivel de stat evidența unică, după cum urmează:

1) instituțiile de învățământ – înregistrează, actualizează, radiază datele despre instituții, clase, grupe, secții, elevi, angajați, utilizatori ai sistemului din cadrul instituțiilor de învățământ în cauză;

2) organele locale de specialitate în domeniul învățământului – înregistrează, actualizează, radiază datele despre organele de specialitate, rețeaua de instituții de învățământ din unitățile

teritorial-administrative în cauză, angajații și utilizatorii sistemului din cadrul organelor de specialitate în cauză;

3) Deținătorul SIME – înregistrează, actualizează, radiază datele despre rețeaua de instituții de învățământ aflate în subordinea MECC, altor organe ale administrației publice centrale, utilizatorii Modulului.

9. Obiectele înregistrării conținute în Modul sunt:

- 1) instituția de învățământ;
- 2) elevul;
- 3) personal didactic;
- 4) personal de conducere;
- 5) personal auxiliar;
- 6) Utilizatorii Modulului.

### **Capitolul III**

## **DREPTURILE, ATRIBUȚIILE ȘI OBLIGAȚIILE PARTICIPANȚILOR LA MODUL**

### **Secțiunea 1**

#### **Drepturile, atribuțiile și obligațiile deținătorului Modulului**

10. Deținătorul are următoarele drepturi:

- 1) să elaboreze și să dezvolte, prin intermediul Cancelariei de Stat, în baza competențelor sale, cadrul normativ cu privire la Modul;
- 2) să propună soluții de perfecționare și eficientizare a procesului de funcționare a Modulului, precum și să le pună în aplicare;
- 3) să supravegheze respectarea cerințelor de securitate a informației de către participanții la Modul, să fixeze cazurile și tentativele de încălcare a acestora;
- 4) să inițieze procedura de revocare a accesului la Modul pentru utilizatorii care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale;
- 5) să verifice autenticitatea și veridicitatea datelor educaționale introduse de participanții la Modul;
- 6) să solicite de la participanți actualizarea sau corectarea datelor Modulului, în caz de depistare a omiterilor și erorilor.

11. Deținătorul are următoarele atribuții:

- 1) asigură condițiile organizatorice și financiare pentru funcționarea Modulului;
  - 2) stabilește scopurile și funcționalitățile Modulului;
  - 3) determină obiectele informaționale supuse înregistrării în Modul și conținutul acestora;
  - 4) asigură securitatea și protecția datelor din Modul;
  - 5) aprobă și coordonează cu administratorul sistemului executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale Modulului, erorile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea normală a acestuia;
  - 6) asigură dezvoltarea continuă a Modulului prin adăugarea de noi componente ce pot fi utilizate de participanți în cadrul Modulului;
  - 7) autorizează, suspendă și revocă dreptul de acces în Modul;
  - 8) stabilește măsurile tehnice și organizatorice de protecție și securitate a Modulului;
  - 9) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a Modulului la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;
  - 10) organizează seminare și instruirii de promovare și utilizare a Modulului pentru utilizatori;
  - 11) asigură acordarea suportului metodologic și tehnic participanților la Modul în procesul de gestionare a resurselor de date educaționale, inclusiv prin elaborarea și menținerea ghidului metodologic privind introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor educaționale, precum și funcționarea Modulului;
  - 12) monitorizează și supraveghează accesările informației din Modul și identifică încălcările comise;
  - 13) exercită alte atribuții necesare asigurării bunei funcționări a Modulului.
12. Deținătorul are următoarele obligații:

- 1) să asigure funcționarea neîntreruptă și ținerea Modulului în conformitate cu cadrul normativ în vigoare;
- 2) să acorde suportul necesar persoanelor autorizate, care au acces la Modul, privind utilizarea complexului de mijloace software aferente acestuia;
- 3) să informeze participanții la Modul despre modificările condițiilor tehnice de funcționare a acestuia;
- 4) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a informației și a datelor cu caracter personal;
- 5) să utilizeze informația obținută din Modul doar în scopurile stabilite de prezentul regulament și cadrul normativ în vigoare.

## **Secțiunea 2**

### **Obligațiile, atribuțiile și drepturile Administratorului național al Modulului**

13. Administratorul național este obligat:
  - 1) să asigure funcționarea și menținerea Modulului în corespundere cu prezentul regulament și actele normative în vigoare;
  - 2) să asigure suportul metodologic și practic pentru toți utilizatorii Modulului cu referire la menținere, actualizarea și utilizarea datelor cu caracter educațional;
  - 3) să asigure colectarea informațiilor, stocarea lor, menținerea și actualizarea Modulului;
  - 4) să verifice, în limita competențelor, veridicitatea informațiilor colectate în Modul;
  - 5) să acorde utilizatorului acces la informația din Modul în conformitate cu prezentul regulament și actele normative în vigoare. În caz de modificare a drepturilor de acces, administratorul trebuie să ia decizia cu privire la reconfigurarea acestora în caz de necesitate;
  - 6) să efectueze, în limitele competențelor, măsurile necesare privind protecția și confidențialitatea informațiilor din Modul, inclusiv împotriva accesului, corectării, modificării și transmiterii neautorizate;
  - 7) să asigure măsurile necesare pentru securitatea cibernetică și a datelor cu caracter personal în corespundere cu actele normative în vigoare;
  - 8) să efectueze monitorizarea activităților utilizatorilor din Modul;
  - 9) să informeze utilizatorii despre modificările organizatorice / tehnice de funcționare a Modulului.
14. Administratorul național are următoarele atribuții:
  - 1) crearea, modificarea, suspendarea/activarea contului pentru participanții la Modul;
  - 2) atribuirea unui rol utilizatorului și/sau unui grup de utilizatori;
  - 3) atribuirea nivelului de acces și aplicarea restricțiilor de acces la datele educaționale;
  - 4) managementul formularelor electronice;
  - 5) managementul șabloanelor de rapoarte și statistici;
  - 6) monitorizarea jurnalizării evenimentelor.
15. Administratorul național are dreptul:
  - 1) să supravegheze respectarea cerințelor de securitate informațională și cibernetică de către utilizatori, să fixeze cazurile și tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea și lichidarea consecințelor, precum și să informeze posesorul SIME;
  - 2) să solicite de la utilizatori colectarea și actualizarea informațiilor în Modul;
  - 3) să inițieze procedura de suspendare și revocare a drepturilor de acces la Modul în cazurile de nerespectare a prezentului regulament și a actelor normative cu privire la securitatea informațională/cibernetică;
  - 4) să stabilească cerințe față de mijloacele tehnice, canalele telecomunicaționale și software la locurile automatizate de muncă ale utilizatorilor;
  - 5) să propună căi suplimentare de perfecționare și eficientizare a funcționării Modulului.

## **Secțiunea a 3-a**

### **Atribuțiile registratorului Modulului**

16. Registratorul Modulului are următoarele atribuții:

- 1) asigură corectitudinea și autenticitatea datelor introduse sau prezentate pentru a fi introduse în Modul;
- 2) transmite către deținător și actualizează informația prezentată cu privire la utilizatori;
- 3) asigură confidențialitatea și autenticitatea datelor transmise spre utilizare în cadrul Modulului;
- 4) raportează deținătorului Modulului problemele de funcționalitate ale acesteia;
- 5) plasează și deține propriile resurse de date educaționale în Modul ;
- 6) asigură calitatea datelor educaționale în Modul în conformitate cu cadrul normativ de profil;
- 7) asigură securitatea informațională a datelor educaționale plasate în Modul;
- 8) utilizează resursele tehnologice comune ale Modulului;
- 9) oferă sugestii de îmbunătățire și contribuie la dezvoltarea continuă a Modulului prin adăugarea de noi componente ce pot fi reutilizate de alți beneficiari la gestionarea datelor în Modul;
- 10) alte atribuții aferente furnizării de date în Modul.

#### **Secțiunea a 4-a**

##### **Obligațiile și drepturile utilizatorilor Modulului**

17. În funcție de rol, utilizatorii Modulului sunt obligați:
  - 1) să asigure înregistrarea, actualizarea, colectarea, prelucrarea și transmiterea informațiilor cu caracter educațional în Modul; conform ghidului metodologic pus la dispoziția utilizatorilor la Modul;
  - 2) să respecte disciplina de înregistrare, evidență și utilizare a informației cu caracter educațional conform actelor normative;
  - 3) să asigure autenticitatea și veridicitatea datelor educaționale introduse în Modul;
  - 4) să asigure și să efectueze controlul sistemului de securitate, să înștiințeze despre cazurile și tentativele de încălcare a acestuia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor;
  - 5) să asigure securitatea accesului la informația conținută în Modul, respectarea condițiilor de securitate și regulilor de exploatare a Modulului;
  - 6) să asigure condițiile necesare pentru păstrarea în siguranță a suporturilor materiale, precum și pentru excluderea accesului terțelor persoane la suporturile respective;
  - 7) să asigure implementarea măsurilor de securitate cibernetică în conformitate cu actele normative;
  - 8) să utilizeze informația obținută din Modul doar în scopurile stabilite de legislația în vigoare și cu respectarea legislației privind dreptul de autor și drepturile conexe;
  - 9) să înștiințeze neîntârziat, în formă verbală și scrisă, administratorul Modulului despre cazurile de încălcare a securității informaționale în conformitate cu actele normative;
  - 10) să aducă la cunoștința deținătorului Modulului , în termen de o zi, orice situație de imposibilitate fortuită de executare (incidente aflate în afara ariei de competență a utilizatorului) care ar putea influența în mod negativ exercitarea funcțiilor utilizatorilor.
  - 11) să aducă la cunoștința Administratorului ierarhic superior despre încetarea raporturilor de muncă/de serviciu.
  - 12) să asigure actualizarea, datelor educaționale introduse în Modul;
  - 13) să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor;
  - 14) să asigure accesul securizat la informația conținută în Modul, respectarea condițiilor de securitate și a regulilor de exploatare a acestuia;
  - 15) să ia măsurile organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu instrucțiunile deținătorului Modulului.
18. Directorii instituțiilor de învățământ primar, gimnazial și liceal sunt obligați:
  - 1) să asigure, să organizeze și să amenajeze locuri de muncă în instituție pentru persoanele responsabile de înregistrarea, actualizarea, colectarea și prelucrarea informației cu caracter educațional.

2) să asigure deservirea tehnică a componentelor și să înlăture defecțiunile tehnice ale locurilor de muncă automatizate conectate la Sistem.

3) să asigure veridicitatea, plenitudinea și actualitatea datelor.

4) să prezinte electronic Administratorului raional/municipal SIME Raportul de confirmare a directorului instituției de învățământ, semnat digital, cu privire la veridicitatea, plenitudinea și actualitatea datelor din Modul. Raportul va fi prezentat la sfârșitul fiecărei perioade de actualizare SIME.

19. Fiecare utilizator are următoarele drepturi:

1) să participe la crearea, implementarea și dezvoltarea Modulului;

2) să inițieze propuneri cu privire la modificarea actelor legislative și normative existente care reglementează funcționarea Modulului;

3) să solicite și să primească gratuit informația cu caracter educațional conținută în Modul, precum și rapoartele statistice generalizate;

4) să solicite și să primească de la administratorul Modulului ajutor metodologic și practic pe problemele ce țin de funcționarea Modulului;

5) să prezinte propuneri administratorului Modulului privind perfecționarea și eficientizarea funcționării Modulului.

6) să participe la implementarea și dezvoltarea Modulului, în limitele drepturilor indicate în prezentul Regulament;

7) să înainteze deținătorului Modulului propuneri privind modificarea și/sau completarea actelor normative care reglementează funcționarea Modulului;

8) să solicite și să primească de la deținătorul Modulului ajutor metodologic și practic privind funcționarea acesteia;

9) să prezinte propuneri deținătorului Modulului privind perfecționarea și eficientizarea funcționării acesteia.

## **Capitolul IV**

### **GESTIONAREA ȘI ASIGURAREA FUNCȚIONĂRII MODULULUI**

20. Modulul se ține în limba de stat, rusă și engleză.

21. Baza de date a Modulului este parte componentă a bazei de date a SIME și asigură evidența centralizată a informației referitoare la instituțiile de învățământ primar și secundar general, elevi, cadre didactice, nedidactice, conducere și auxiliare, precum și eliberarea rapoartelor statistice generalizate privind starea Modulului.

22. Introducerea datelor în Modul se efectuează în baza documentelor primare sau din alte sisteme informaționale, care conțin datele educaționale necesare.

23. Evidența obiectelor informaționale se ține conform metodologiilor coordonate/ aprobate de către posesorul Sistemului.

24. În cazul depistării unor erori sau inexactități în datele introduse, utilizatorii Modulului sunt obligați să informeze despre aceasta administratorul de rang mai înalt, care va asigura eliminarea acestora din Modul.

25. Dacă furnizorul datelor Modulului nu are drepturile necesare pentru a corecta erorile în sistem, se va adresa la nivelul superior printr-o solicitare argumentată privind rectificarea datelor eronate sau inexacte.

26. Radierea datelor din Modul se efectuează de către administratorul Modulului în baza deciziei registratorului, cu respectarea strictă a cerințelor privind protecția datelor cu caracter personal. Radierea datelor se face prin inserarea unei note speciale și nu reprezintă excluderea fizică a datelor din Modul.

27. Funcționarea Modulului este asigurată de deținător până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării Modulului, datele și documentele conținute în acesta se transmit în arhivă conform actelor normative.

28. Datele din Modul ce dezvăluie originea etnică a persoanei, apartenența socială și datele privind starea de sănătate fac parte din categoria specială a datelor cu caracter personal. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul Modulului se efectuează cu respectarea strictă a actelor normative.

29. Accesul la Modul se realizează în regim eficient și neîntrerupt.

30. Perioadele de actualizare a datelor sunt stabilite de Ministerul Educației, Culturii și Cercetării prin ordine aprobate.

31. Confirmarea veridicității datelor introduse în modul, va fi efectuată prin aplicarea semnăturii electronice de către administratorul instituției.

## **Capitolul V**

### **REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN MODUL**

#### **Secțiunea 1**

##### **Acordarea dreptului de acces la Modul**

32. Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea numelui, prenumelui, IDNP-ului, funcției, e-mailului personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

33. Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective. Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces, întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

34. Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.

35. Accesul la datele din Modul se acordă în conformitate cu actele normative privind accesul la informație. Utilizatorii beneficiază de drepturi egale de acces la informația din Modul, în limitele rolurilor atribuite și nu sunt obligați să justifice, în fața posesorului/deținătorului Modulului, necesitatea obținerii informației solicitate, cu excepția datelor cu caracter personal.

36. Accesul la funcționalitățile Modulului este condiționat de rolul utilizatorului.

37. Utilizatorii au drept de acces la informația din Modul conform atribuțiilor și funcțiilor deținute și regimului juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și/sau profilului de acces.

38. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

39. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

40. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

41. Participanții au drept de acces la informația din Modul conform atribuțiilor și funcțiilor deținute și regimului juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și/sau profilului de acces.

42. Informația conținută în Modul se divizează în:

1) informații publice accesibile tuturor utilizatorilor, inclusiv a informației de pe interfața Modulului, care pot fi accesate fără necesitatea autentificării în sistem;

2) informații cu acces limitat, care sunt puse la dispoziția angajaților entităților publice și a utilizatorilor privați care, pentru accesare, necesită autentificare în sistem.

43. La înregistrarea în cadrul Modulului, fiecărui utilizator i se atribuie un identificator unic și rolul de care depinde dreptul de acces la obiectele informaționale. Autorizarea utilizatorilor se produce în conformitate cu nivelul de acces stabilit și utilizatorii au posibilitatea să acceseze funcționalitățile sau informațiile disponibile potrivit nivelului de acces.

44. La baza mecanismului de autentificare în cadrul Modulului se află serviciul electronic guvernamental de autentificare și control al accesului (MPass). Utilizatorii care nu au semnătură electronică vor putea fi autentificați în Modul în baza de nume și parolă, oferite de către deținător.

45. Dreptul de acces la resursele informaționale ale Modulului este segmentat pe unități de conținut, atribuind prerogative partajate, și anume: vizualizare, adăugare, redactare și ștergere.

46. Accesul la resursele informaționale ale Modulului este segmentat pentru utilizatorii interni și utilizatorii externi.

47. Utilizatori interni ai Modulului sunt deținătorul Modulului și administratorul de sistem, ale căror drepturi de acces sunt definite în prezentul Regulament și alte acte normative.

48. Posesorul Modulului are acces cu drept de vizualizare a datelor din Modul, în limita scopului și atribuțiilor acordate prin prezentul Regulament și cadrul normativ în vigoare.

49. Accesul la datele platformei se realizează prin:

- 1) acordarea accesului public la informația nerestricționată, plasată pe Modul;
- 2) acordarea accesului utilizatorilor externi, în limitele prezentului Regulament;
- 3) acordarea accesului utilizatorilor interni, precum și registratorilor din cadrul entităților juridice, în limitele competențelor.

50. La acordarea accesului utilizatorilor la datele educaționale, utilizatorul acestora asigură respectarea legislației privind dreptul de autor și drepturile conexe.

51. Exploatarea Modulului fără autorizare nominală este strict interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public.

52. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

53. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

54. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

## **Secțiunea a 2-a**

### **Revocarea dreptului de acces în Modul**

55. Dreptul de acces la Modul nu este unul permanent și poate fi revocat în circumstanțele prevăzute de prezentul Regulament. Introducerea și/sau modificarea datelor din Modul de pe un nume sau profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Participanții la Modul urmează să se asigure că profilul de utilizator, precum și semnătura electronică sunt confidențiale.

56. Revocarea dreptului de acces la Modul se efectuează de deținător, în una din următoarele situații:

- 1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale registratorului/utilizatorului Modulului;
- 2) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților registratorului/utilizatorului, când noile atribuții nu impun accesul la datele Modulului;
- 3) la suspendarea/expirarea/rezilierea sau revocarea contractului de prestări servicii educaționale încheiat între deținătorul și utilizatorul datelor educaționale;
- 4) în alte cazuri, în limitele legislației.

57. Revocarea dreptului de acces la Modul se poate efectua de către deținătorul Modulului, în una din următoarele situații:

- 1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale angajaților deținătorului Modulului;
- 2) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților deținătorului Modulului, când noile atribuții nu impun accesul la datele Modulului;
- 3) la încălcarea regulilor de utilizare a sistemului sau la constatarea încălcării securității informaționale de către utilizatori;
- 4) la cererea expresă a participanților la Modul, pentru sine sau utilizatorii săi de date educaționale;
- 5) în alte cazuri, în limitele legislației.

58. Accesul la datele din Modul se acordă în conformitate cu actele normative privind accesul la informație. Utilizatorii beneficiază de drepturi egale de acces la informația din Modul, în limitele rolurilor atribuite și nu sunt obligați să justifice, în fața posesorului/deținătorului Modulului, necesitatea obținerii informației solicitate, cu excepția datelor cu caracter personal.

59. Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea

numelui, prenumelui, IDNP-ului, funcției, e-mailul personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

60. Revocarea dreptului de acces la Modul pentru utilizatori se efectuează în una dintre următoarele situații:

- 1) în temeiul notificării conducătorului acestuia;
- 2) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;
- 3) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele din Modul;
- 4) la constatarea încălcării de către utilizator a prezentului regulament.

61. Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective.

62. Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

63. Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.

64. Se interzice utilizarea datelor din Modul în scopuri contrare prezentului regulament și actelor normative în vigoare.

65. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul actelor normative în vigoare privind protecția datelor cu caracter personal.

66. Destinatarul datelor nu este în drept să modifice datele obținute din Modul, iar la utilizarea acestora este obligat să indice sursa lor.

## **Capitolul VI**

### **INTERACȚIUNEA CU ALTE SERVICII ȘI PLATFORME ELECTRONICE GUVERNAMENTALE**

67. Modulul este găzduit pe platforma tehnologică guvernamentală comună (MCloud), care permite accesul, la cerere, pe bază de rețea, la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu: rețele, servere echipamente de stocare, aplicații și servicii) ce pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, sistemul poate fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

68. Modulul utilizează următoarele servicii electronice și platforme guvernamentale:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 1090/2013 „Privind serviciul electronic guvernamental de autentificare și control al accesului (MPass)”;

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 405/2014 „Privind serviciul electronic guvernamental integrat de semnătură electronică (MSign)”;

3) serviciul electronic guvernamental de jurnalizare (MLog) – instrument securizat și flexibil de jurnalizare și audit, utilizat pentru asigurarea evidenței operațiunilor (evenimentelor) produse în SIME și registrele formate de acesta.

## **Capitolul VII**

### **Secțiunea 1** **Securitatea informației în Modul**

69. Serviciile furnizate de Modul se conformează cerințelor minime de securitate corespunzătoare cerințelor de securitate a aplicațiilor livrate din platforma MCloud.

70. Măsurile de protecție și securitate a informației cu caracter educațional din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIME și se efectuează neîntrerupt de către toți utilizatorii.

71. Protecția informației din Modul se efectuează prin următoarele metode:

- 1) folosirea metodelor de cifrare și criptare a informațiilor din Modul;
- 2) prevenirea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor sau defecțiuni în funcționarea complexului tehnic și de program, asigurată prin metoda folosirii mijloacelor de protecție speciale de program, antivirus și efectuarea periodică a copiilor de rezervă.

72. Fiecare instituție elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională și cibernetică pentru asigurarea respectării prezentului regulament și a actelor normative în vigoare.

73. Fiecare instituție desemnează o persoană responsabilă de actualizarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională și cibernetică.

74. Administratorii și operatorii subdiviziunilor structurale pot efectua acțiuni de introducere, modificare, păstrare și extragere a informațiilor cu caracter educațional care se referă doar la unitatea administrativ-teritorială, instituția sau clasa de care sunt responsabili.

75. Analistii nu au acces la datele cu caracter personal și pot efectua doar acțiuni de vizualizare și extragere a informațiilor statistice, referitoare la unitatea administrativ-teritorială sau instituția de care sunt responsabili.

76. Măsurile de protecție și securitate a informației cu caracter personal din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a Modulului și se efectuează neîntrerupt de către toți participanții.

77. Obiecte ale asigurării protecției și securității informației din Modul se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

- 1) platforma guvernamentală, sistemele operaționale, sistemele de gestiune a Modulului, sistemele de evidență și alte aplicații care asigură funcționarea Modulului;
- 2) sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

78. Protecția informației cu caracter personal în Modul la nivel de deținător ale acesteia se efectuează prin următoarele metode:

- 1) asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport date;
- 2) excluderea accesului neautorizat la datele din Modul prin utilizarea funcționalităților de autorizare ale serviciului MPass;
- 3) prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau cauzează defecțiuni în funcționarea complexului tehnic și de program;
- 4) efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;
- 5) efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării Registrului în cazul incidentelor.

79. Protecția informației cu caracter personal la nivel de participant la Modul se efectuează prin următoarele metode:

- 1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor din Modul;
- 2) monitorizarea procesului de exploatare a Modulului prin intermediul mecanismului de jurnalizare efectuat de deținătorul acesteia.

80. Participanții la Modul elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, incluzând:

- 1) identitatea persoanei responsabile de politica de securitate;
- 2) principalele măsuri tehnico-organizatorice necesare asigurării funcționării Modulului;
- 3) procedurile interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din Modul;
- 4) responsabilitățile personalului participantului la Modul privind asigurarea securității informaționale;

5) procedurile de control intern al participantului la Modul privind respectarea condițiilor de securitate informațională.

81. Fiecare participant la Modul asigură informarea sau, după caz, instruirea utilizatorilor privind metodele și procedeele de contracarare a pericolelor informaționale.

## **Secțiunea a 2-a**

### **Protecția datelor cu caracter personal din Modul**

82. Datele de autentificare în Modul fac parte din categoria datelor cu caracter personal. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul Modulului se efectuează de către subiecții cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

83. Măsurile de protecție și securitate a informației cu caracter educațional din Modul reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIME și se efectuează neîntrerupt de către toți utilizatorii.

84. Protecția informației din Modul se efectuează prin următoarele metode:

- 1) folosirea metodelor de cifrare și criptare a informațiilor din Modul;
- 2) prevenirea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor sau defecțiuni în funcționarea complexului tehnic și de program, asigurată prin metoda folosirii mijloacelor de protecție speciale de program, antivirus și efectuarea periodică a copiilor de rezervă.

85. Fiecare instituție elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională și cibernetică pentru asigurarea respectării prezentului regulament și a actelor normative în vigoare.

86. Fiecare instituție desemnează o persoană responsabilă de actualizarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională și cibernetică.

87. Administratorii și operatorii subdiviziunilor structurale pot efectua acțiuni de introducere, modificare, păstrare și extragere a informațiilor cu caracter educațional care se referă doar la unitatea administrativ-teritorială, instituția sau clasa de care sunt responsabili.

88. Analistii nu au acces la datele cu caracter personal și pot efectua doar acțiuni de vizualizare și extragere a informațiilor statistice, referitoare la unitatea administrativ-teritorială sau instituția de care sunt responsabili.

## **Capitolul VIII**

### **SUSPENDAREA FUNCȚIONĂRII MODULULUI**

89. Pentru asigurarea funcționalității eficiente și neîntrerupte, schimbul informațional de date în Modul este asigurat în regim non-stop.

90. Funcționarea Modulului se suspendă de către administratorul tehnic, după coordonarea prealabilă cu deținătorul Modulului, în cazul apariției uneia dintre următoarele situații:

- 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al Modulului;
- 2) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea Modulului;
- 3) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al Modulului;
- 4) la cererea scrisă a posesorului Modulului.

91. Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea, în scris sau prin e-mail, a furnizorilor de resurse de instruire de către deținătorul Modulului, în baza planului coordonat cu administratorul tehnic, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea furnizorilor de resurse de instruire și coordonarea prealabilă cu deținătorul Modulului, în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware. Dacă lucrările profilactice durează mai mult de 5 de zile, la expirarea fiecărei perioade de 5 de zile de efectuare a lucrărilor, se notifică Furnizorii.

92. Furnizarea serviciilor oferite de Modul poate fi suspendată de către administratorul tehnic fără consimțământul deținătorului Modulului, cu notificarea ulterioară a acestuia, în următoarele situații:

- 1) situații de incidente la scară;
- 2) la apariția situațiilor de imposibilitate fortuită de executare;
- 3) situații de criză.

93. Suspendarea serviciilor se efectuează asigurându-se un impact minim asupra calității serviciilor livrate furnizorilor de resurse de instruire și utilizatorilor acestora.

## **Capitolul IX MONITORIZARE ȘI CONTROL**

### **Secțiunea 1 Controlul extern**

94. Menținerea Modulului este supusă controlului intern, extern și sub aspectul legalității operațiunilor de prelucrare a datelor cu caracter personal. Controlul extern asupra respectării cerințelor privind crearea, menținerea, exploatarea și reorganizarea Modulului poate fi efectuată de către autoritățile împuternicite.

95. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal în cadrul Modulului se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter personal al Republicii Moldova.

96. La efectuarea controlului extern, organul de control alcătuiește un raport privind controlul extern. Deținătorul Modulului este obligat să ia măsuri pentru lichidarea încălcărilor identificate și să informeze despre aceasta organul de control.

97. Pentru organizarea controlului de funcționare a Modulului este responsabil deținătorul Modulului/administratorul tehnic, care este obligat să asigure dreptul de acces la Modul și mijloacele de ținere a acestuia, respectiv în încăperile în care se află mijloacele hardware utilizate în acest scop.

98. Participanții responsabili de asigurarea funcționării Modulului și înregistrării datelor poartă răspundere personală, în conformitate cu cadrul normativ, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.

99. Toți participanții la Modul și destinatarii informațiilor ce conțin date cu caracter personal poartă răspundere conform legislației în vigoare pentru divulgarea, transmiterea acestora persoanelor terțe și pentru utilizarea lor în scopuri personale.

100. Funcționarea Modulului este asigurată de deținătorul Modulului până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

### **Secțiunea a 2-a Monitorizarea și controlul intern**

101. Controlul intern privind organizarea și funcționarea Modulului se efectuează de către posesorul SIME.

102. Responsabilitatea pentru organizarea și funcționarea Modulului se atribuie administratorului acestuia, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea Modulului. Actele elaborate se coordonează cu posesorul SIME.

103. Persoanele cu funcții de răspundere, în obligațiile cărora intră menținerea Modulului, furnizarea informațiilor din Modul, precum și asigurarea funcționării Modulului, poartă răspundere personală pentru plenitudinea, autenticitatea, veridicitatea, integritatea informațiilor, precum și pentru păstrarea și utilizarea lor. În caz de încălcare, aceștia pot fi trași, potrivit legii, la răspundere disciplinară, civilă, contravențională și/sau penală.

104. În scopul monitorizării și controlului asupra executării Regulamentului, cooperarea dintre posesorul platformei și furnizorul de resurse de instruire va fi asigurată prin schimb de informație, raportare periodică, ședințe comune de evaluare, replanificare, audit etc.

105. Concluziile generate de eforturile de monitorizare, control și evaluare sistematică vor servi drept bază în luarea deciziilor corective pe parcursul implementării platformei, planificarea activităților la diferite etape de operare a platformei, evaluarea performanței participanților la utilizarea platformei, supravegherea procesului de implementare și operare a resurselor informaționale elaborate pe baza platformei etc.

106. Accesul la informația din Modul, pentru utilizatori, se acordă de către administratori, în limitele rolurilor atribuite și domeniului de vizibilitate, în baza actului normativ, cu specificarea numelui, prenumelui, IDNP-ului, funcției, email-ul personal de serviciu, numărul de telefon mobil și fix, rolul solicitat și termenul de acordare a rolului.

107. Revocarea dreptului de acces la Modulul pentru utilizatori se efectuează în una dintre următoarele situații:

- 1) în temeiul notificării conducătorului acestuia;
- 2) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;
- 3) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele din Modul;
- 4) la constatarea încălcării de către utilizator a prezentului regulament.

108. Sesizarea constatării încălcării de către utilizatorul Modulului, a securității informaționale și cibernetice, se realizează, după caz, de către administratorii și persoanele responsabile de politica de securitate printr-o notă de serviciu adresată conducătorului instituției respective.

109. Conducătorul instituției, în funcție de gravitatea încălcării și gradul de vinovăție al utilizatorului ce a comis încălcarea, va decide dacă revocă sau nu dreptul de acces întreprinderea măsurilor de remediere a posibilelor lacune în instruire a utilizatorului, de informare a organelor cu competențe în investigarea infracțiunilor informatice și/sau de protecție a datelor cu caracter personal.

110. Restabilirea dreptului de acces la Modul pentru utilizatorul căruia i-a fost revocat acest acces se poate face potrivit regulilor generale prevăzute de prezentul Regulament.