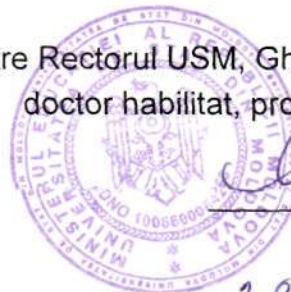


MINISTERUL EDUCAȚIEI AL REPUBLICII MOLDOVA  
UNIVERSITATEA DE STAT DIN MOLDOVA  
SECȚIA RESURSE UMANE

Aprobat

De către Rectorul USM, Gheorghe Ciocanu  
doctor habilitat, profesor universitar



28.04.2015

REGULAMENTUL  
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE  
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ A  
SALARIAȚILOR UNIVERSITĂȚII DE STAT DIN MOLDOVA  
(USM)

## **I. DISPOZIȚII GENERALE**

- 1.1. Prezentul Regulament are ca scop procedurile și mecanismele de implementare la nivel de unitate a prevederilor Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, a Hotărîrii Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal” și întru respectarea prevederilor art. 91 – 94 ale Codului muncii al Republicii Moldova.
- 1.2. În vederea implementării cadrului legislativ în vigoare și conformarea față de prevederile acestuia, USM adoptă prezentul Regulament și urmează să se conducă de prevederile acestuia în orice situație legată de prelucrarea datelor cu caracter personal a salariaților săi, avînd în vedere în special activitățile de prelucrare a informațiilor conținute sau derivate din buletinul de identitate a salariatului sau un alt act de identitate a acestuia, carnetul de muncă, documentele de evidență militară, certificate de stare civilă, certificat de atribuire a Codului Personal de Asigurări Sociale, certificatul medical, diploma de studii, cv, autobiografice, informațiile despre salariu și din alte acte colectate pe parcursul existenței raporturilor juridice între părți.
- 1.3. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale salariaților USM în cadrul sistemului de evidență a salariaților USM.

## **II. PRINCIPIILE ȘI SCOPUL ACTIVITĂȚII DE PRELUCRARE A DATELOR CU CARACTER PERSONAL**

- 2.1. USM recunoaște și respectă drepturile și libertățile salariaților săi, astfel ca prelucrarea datelor cu caracter personal să se desfășoare în conformitate cu prevederile actelor legislative în vigoare precizate la punctul I (1.1) din prezentul Regulament.
- 2.2. Prelucrarea datelor cu caracter personal a salariaților este necesară pentru perfectarea actelor de angajare, asigurarea evidenței salariaților și raporturilor de muncă avute cu aceștia, perfectarea actelor obligatorii pentru evidența salarială, asigurare medicală, asigurare socială, evidență fiscală, asigurarea transferurilor bancare, perfectarea salariilor și retribuirea muncii, aplicarea de mențiuni, sancțiuni, și altor scopuri necesare activității de evidență și monitorizare a raporturilor salariale.
- 2.3. Datele cu caracter personal a salariaților angajați în cadrul USM pot fi comunicate doar subiectului vizat, sau terților împuterniciți de către acesta sau subiecților expres prevăzuți de lege.
- 2.4. În calitate de operator de date cu caracter personal USM are obligația de a administra în condiții de siguranță și numai pentru scopurile specificate, datele personale furnizate de salariați, ori de un membru de familie al acestora.

2.5. În cadrul sistemului de evidență a Salariaților USM sînt prelucrate următoarele categorii de date cu caracter personal:

- \* numele, prenumele și patronimicul
- \* sexul
- \* data și locul nașterii
- \* IDNP (număr personal de identificare de stat)
- \* cetățenia
- \* formarea profesională/studii/diplome
- \* date ale membrilor de familie
- \* CPAM (cod personal de asigurare medicală)
- \* CPAS (cod personal de asigurare socială)
- \* date despre situația și evidența militară
- \* date din permisul de conducere (numai în cazul angajării în funcție de șoferi)
- \* loc de muncă
- \* sancțiuni disciplinare
- \* adresa la domiciliu/reședința
- \* telefon/email
- \* starea sănătății (*art. 92, lit. e) din CM - numai în cazul determinării capacității salariatului de a-și îndeplini obligațiile de funcție*)
- \* semnătura
- \* imaginea (foto)

### III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ A SALARIAȚILOR

3.1. Sistemul de evidență a salariaților include totalitatea informațiilor despre salariați necesară pentru perfectarea actelor de angajare, asigurarea evidenței salariaților și raporturilor de muncă avute cu aceștia, perfectarea actelor obligatorii pentru evidența salarială, asigurare medicală, asigurare socială, evidență fiscală, asigurarea transferurilor bancare, perfectarea salariilor și retribuirea muncii, aplicarea de mențiuni, sancțiuni, și altor scopuri necesare activității de evidență și monitorizare a raporturilor salariale.

3.2. Datele cu caracter personal conținute în sistemul de evidență al salariaților USM se prelucrează/stochează:

1. pe suport de hîrtie;
2. în format electronic:
  - a) Software – Sistemul de evidență al salariaților USM care este instalat la computerul central – „Șef secția resurse umane și cu drept de acces la al doilea computer – „Materiale”, computerele aflîndu-se în biroul 110, 123,125 din sediul USM ;

b) Hardware – calculator nr de inventariere **biroul 110** 00-001489, 00-000608, 00-001492, 00-001491; **biroul 123** 00-001493, 00-001494; **biroul 125** 00-001490.

3.3. Mentenanța programului este efectuată de către compania **A.O. RENAM**, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între USM și compania **A.O. RENAM**, cu următoarele atribuții stabilite companiei prestatoare:

- Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului (Linia fierbinte);
- Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

3.4. Prelucrarea informațiilor în sistemul de evidență a salariaților pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sînt amplasate fizic în biroul 110,123 din sediul USM.

#### **IV. MODALITATEA DE PRELUCRARE A DATELOR CU CARACTER PERSONAL ÎN CADRUL SISTEMULUI DE EVIDENȚĂ A SALARIAȚILOR**

4.1. Temei de includere a informației personale în sistemul de evidență a salariaților USM servește cererea de angajare și contractul individual de muncă care este perfectat la solicitarea salariatului și în urma semnării căruia poate fi inițiată de către Secția Resurse Umane procedura de formare a dosarului personal al salariatului, care urmează să conțină actele stipulate de prevederile art. 57 din Codul Munci, după cum urmează:

- \* copia buletinului de identitate
- \* carnetul de muncă
- \* adeverința de recrut sau livretul militar (*se înregistrează în secția de evidență militară*)
- \* copii ale diplomelor, certificatelor de studii, calificare
- \* fișa personală – Formular interdepartamental tipizat MR-2
- \* fișa personală de evidență a cadrelor cu imagine (*p/u persoanele care participă la concursul p/u ocuparea posturilor didactice și de conducere vacante*)
- \* certificat medical (art. 92, lit. e) din CM - numai în cazul determinării capacității salariatului de a-și îndeplini obligațiile de funcție)
- \* CPAM (cod personal de asigurare medicală)
- \* CPAS (cod personal de asigurare socială)

4.2. Informațiile despre salariați, care conțin date cu caracter personal prelucrate în cadrul Secției Resurse Umane urmează a fi stocate cu respectarea prevederilor art.4, alin.(1) lit. e) din Legea nr.133, pe durata necesară realizării scopurilor în vederea cărora au fost colectate și ulterior prelucrate cu respectarea drepturilor subiectului, în special a dreptului de acces, de intervenție și de opoziție.

4.3. După expirarea termenului de stocare, prelucrare a datelor, în cazul USM expirarea/rezilierea contractului individual de muncă al salariaților, dosarele

cu materialele stocate pe suport de hîrtie se transmit printr-un proces verbal de predare-primire de cître angajații Secției Resurse Umane în arhiva universității, unde urmează a fi păstrate ca documente de arhivă pe durata stabilită prin "Indicatorul documentelor-tip și al termenelor de păstrare pentru organele administrației publice, pentru instituții și întreprinderile RM".

## V. DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR

- 5.1. USM în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților garantîndu-le asigurarea drepturilor stabilite spre asigurare de cadrul legal în vigoare subiecților vizati, precum și, după caz, altor persoane vizate sau terți.
- 5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.
- 5.3. Vor avea calitatea de persoane împuternicite cu drept de administrare și/sau prelucrare a informațiilor din sistemul de evidență a salariaților USM doar inspectorii angajați în cadrul Secției Resurse Umane al USM și care au ca atribuții în fișa de post colectarea, utilizarea, prelucrarea, datelor cu caracter personal.
- 5.4. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență a salariaților USM vor respecta procedura de acces la datele cu caracter personal revăzută de prezentul Regulament și cadrul legal în vigoare.
- 5.5. Angajații Secției Resurse Umane vor utiliza datele cu caracter personal ale persoanelor - subiecți ai datelor cu caracter personal prin intermediul unei cereri completate manual (cartotecă cu fișe personale – Formular interdepartamental tipizat MR-2, Fișa personală de evidență a cadrelor), alcătuite din informații obținute direct de la subiecți prin consimțămîntul acestora.
- 5.6. Prelucrarea datelor cu caracter personal se efectuează nemijlocit cu Consimțămîntul subiectului, pentru angajați se exprimă prin semnarea Contractului individual de muncă, în care art. 9, 10, 11 stipulează că Salariatul este informat asupra drepturilor sale stipulate în Legea nr. 133 din 08.07.2011.
- 5.7. Nu este necesar Consimțămîntul subiectului în următoarele cazuri:
  - a) cînd prelucrarea este necesară în vederea protejării vieții sau sănătății persoanei subiect al datelor cu caracter personal (prezentarea datelor personale la Compania Națională de Asigurări în Medicină pentru perfectarea poliței de asigurări medicale);
  - b) cînd prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului (prezentarea datelor personale pentru perfectarea CPAS la CNAS, centrele militare).
  - c) cînd prelucrarea este necesară în vederea comunicării datelor unor autorități publice în cadrul unei competențe speciale de anchetă (de ex.

datele personale solicitate de instanțele de judecată, procurori, organe de urmărire penală, dacă sunt necesare desfășurării unei anchete).

În baza cadrului legal, operatorul, la solicitarea informației de către subiect, poate comunica date referitoare la: identitatea operatorului, categoriile de date cu caracter personal pe care le prelucrează, scopurile prelucrării, precum și dacă unui destinatar terț i-au fost dezvăluite aceste date.

- 5.8. Prin cerere, subiecții datelor cu caracter personal au dreptul să se informeze despre modul și mecanismul de prelucrare a datelor proprii de către operator.
- 5.9. Subiecții datelor cu caracter personal au dreptul de a solicita de la operator: verificarea exactității și a caracterului complet al datelor cu caracter personal care îi privesc; rectificarea, actualizarea blocarea sau ștergerea datelor cu caracter personal a căror prelucrare contravine Legii nr. 133/08.07.2011.
- 5.10. Subiecții datelor cu caracter personal ai USM au dreptul de a se opune, în mod gratuit, în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca datele care îi vizează să facă obiectul unei prelucrări, cu excepția cazurilor prevăzute de legislație. În caz de opoziție justificată prelucrarea datelor în cauză nu mai poate avea loc.
- 5.11. Subiecții datelor cu caracter personal ai USM au dreptul de a se opune, în orice moment, în mod gratuit și fără nici o justificare, ca datele care îi vizează să fie prelucrate în scop de marketing, în numele operatorului, sau să fie dezvăluite unor terți într-un asemenea scop.
- 5.12. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii USM. Informațiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.
- 5.13. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.
- 5.14. Operatorul este obligat să reacționeze și să soluționeze plîngerile, petițiile și orice alte cereri legate de prelucrarea datelor cu caracter personal, în termenele și condițiile prevăzute de lege.

## **VI. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL**

- 6.1. Angajații Secției Resurse Umane deținători de date cu caracter personal, reieșind din specificul activității, elaborează și organizează implementarea prevederilor regulamentului care stabilește politica de securitate a datelor cu caracter personal, inclusiv procedurile și măsurile legate de realizarea acestei politici.
- 6.2. Obiectivele principale ale politicii de securitate sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu

caracter personal prelucrate de către angajații Secției Resurse Umane, atât în cadrul prelucrării manuale, cât și sistemelor informaționale.

- 6.3. Angajații Secției Resurse Umane deținători ai baze de date vor asigura protecția datelor cu caracter personal prin aplicarea corespunzătoare a legislației în vigoare cu referire la protecția datelor și confidențialitatea comunicării.
- 6.4. Politica de securitate, în mod obligatoriu va fi adusă la cunoștință sub semnătura tuturor angajaților Secției Resurse Umane responsabil de prelucrarea datelor cu caracter personal înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.
- 6.5. Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoștința utilizatorilor și altor salariați ai deținătorului de date cu caracter personal, în limitele competențelor funcționale și nivelului de acces acordat.
- 6.6. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.
- 6.7. Prezentul regulament se revizuește cel puțin o dată în an, ca rezultat al modificărilor sau reevaluării componentelor acestuia și aprobat la cel mai înalt organ suprem de conducere al instituției – Senatul Universității de Stat din Moldova.

## **VII. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL ȘI MECANISMELE DE PUNERE ÎN APLICARE A ACESTORA**

- 7.1. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul informațional de date cu caracter personal, se desfășurează ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.
  - a) Registrele salariaților ținute în formă manuală care conțin date cu caracter personal se păstrează în safeul Secției Resurse Umane.
  - b) Registrele în formă electronică a salariilor se păstrează în Secția Resurse Umane. Accesul la registrele ținute în formă electronică este acordat doar persoanelor autorizate de către operator, și se efectuează prin parole individuale, calitative, în mărime de minimum 8 /opt/ simboluri, care nu sunt legate de informația cu caracter personal a deținătorului de date cu caracter personal, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere. Modificarea parolilor se efectuează cu regularitate, la intervale de maximum 3 /trei/ luni și accesul altor persoane este strict interzis.

- c) Protecția externă a datelor cu caracter personal ale salariaților se realizează prin intermediul serviciului de pază, mijloacelor de supraveghere video, semnalizare și alarmă antiincendiară.
- 7.2. Sunt supuse protecției toate resursele informaționale, care conțin date cu caracter personal, inclusiv:
- a) suporturile pe hârtie (registru de evidență a salariaților, dosarele personale ce conțin date cu caracter personal ale salariaților, și alte baze de date).
  - b) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
  - c) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, mijloacele de confecționare și multiplicare a documentelor, alte mijloace tehnice de prelucrare a informației.
- 7.3. Protecția datelor cu caracter personal în sistemul informațional al USM este asigurată în scopul:
- a) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
  - b) preîntâmpinării distrugerii, modificării, copierii;
  - c) respectării cadrului normativ de operare a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
  - d) asigurării caracterului complet, integru și veridic al datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
  - e) asigurării posibilității de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.
- 7.4. Protecția datelor cu caracter personal prelucrate în sistemul informațional al USM se efectuează prin următoarele măsuri:
- a) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
  - b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
  - c) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul sistemului tehnic și de program;
  - d) preîntâmpinarea acțiunilor intenționate și/sau neintenționate ale utilizatorilor interni și/sau externi, precum și ale altor deținători de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul sistemului tehnic și de program.
- 7.5. Preîntâmpinarea scurgerii informațiilor care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim, iar preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță.



- 7.6. Mecanismul de punere în aplicare a măsurilor de protecție este asigurat prin separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale, prin izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea acestui sistem și posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităților, a folosirii resurselor informaționale în care sunt prelucrate datele cu caracter personal.
- 7.7. Acces la bazele de date vor avea numai persoanele autorizate- angajați ai Secției Resurse Umane și numai la îndeplinirea obligațiilor de serviciu, iar copierea datelor se va putea face numai la locul în care sunt gestionate. Fiecare dintre inspectorii serviciului resurse umane- utilizatori de date, accesează numai acea bază de date pe care o are în gestiune:
- a) utilizatorii care au acces la baza de date cu caracter personal sunt doar din conducerea universității (rector, prorectori, decani). Toți utilizatorii sunt obligați să păstreze confidențialitatea datelor la care au acces, iar la finele fiecărei sesiuni de prelucrare a datelor să asigure integritatea și păstrarea lor în locul stabilit.
  - b) copierea sau imprimarea datelor cu caracter personal se realizează numai de către inspectorii – utilizatori autorizați pentru această operațiune și numai în scopuri cerute de legile în vigoare ( copii la buletine de identitate, CPAS, polițe medicale).
  - c) este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
  - d) corespondența (scrisori, certificate, etc.), care conține date cu caracter personal, se marchează, indicându-se prescripții pentru prelucrarea ulterioară și răspîndirea acesteia, inclusiv indicându-se numărul de identificare unic al USM ca operator de date cu caracter personal.
  - e) în cazul în care dezvăluirea datelor este impusă de lege ( de exemplu, în vederea executării unei hotărîri judecătorești), angajații Secției Resurse Umane se vor asigura că terțul care solicită dezvăluirea acționează în conformitate cu prevederile legislației în vigoare.
- 7.8. Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale ce conțin date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului sistemelor informaționale.
- 7.9. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează datele cu caracter personal, totodată asigurîndu-se integritatea și confidențialitatea datelor cu caracter personal transmise prin utilizarea mijloacelor de protecție criptografică a informației și semnătura digitală.

## **VIII. IDENTIFICAREA, AUTENTIFICAREA ȘI ADMINISTRAREA ACCESULUI UTILIZATORULUI ÎN SISTEMUL INFORMAȚIONAL DE DATE CU CARACTER PERSONAL**

- 8.1. În scopul identificării cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal, operatorul înregistrează și se duce

evidența persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal.

- 8.2. Toți utilizatorii Secției Resurse Umane dețin un identificator personal – ID-ul utilizatorului, pentru confirmarea căruia sunt utilizate parole și mijloace fizice speciale de acces cu memorie.
- 8.3. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea parolelor pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acestora. La momentul introducerii, parolele nu se reflectă în clar pe monitor. Angajații Secției Resurse Umane vor modifica parolele de fiecare dată când va depista indici ai unei eventuale compromiteri a sistemului sau parolei.
- 8.4. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sunt folosite identificatoare și parole individuale ale acestora. Operatorul asigură utilizatorilor posibilitatea de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare accesul este blocat. Operatorul asigură, pentru o perioadă de 1 /un/ an păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.
- 8.5. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în cazul de modificare a drepturilor de acces ale utilizatorului, abuz a utilizatorului de codurile primite în scopul comiterii unei fapte prejudiciabile, absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă.
- 8.6. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizate, operatorul revizuire cu regularitate, maximum peste fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul informațional de date cu caracter personal.

## **IX. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ SECȚIA RESURSE UMANE**

- 9.1. Se organizează generarea înregistrărilor de audit a securității în sistemul automatizat de evidență a salariilor pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
- 9.2. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
  - a) data și timpul tentativei intrării/ieșirii;
  - b) ID-ul utilizatorului;
  - c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.

- 9.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemul automatizat de evidență a salariaților, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
- a) data și timpul tentativei de pornire;
  - b) denumirea/identificatorul programului aplicativ sau al procesului;
  - c) ID-ul utilizatorului;
  - d) rezultatul tentativei de pornire – pozitivă sau negativă.
- 9.4. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul de sistemul automatizat de evidență a salariaților, conform următorilor parametri:
- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
  - b) denumirea (identificatorul) aplicației sau a procesului;
  - c) ID-ul utilizatorului;
  - d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
  - e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
  - f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.
- 9.5. Se efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- a) data și timpul modificării competențelor;
  - b) ID-ul administratorului care a efectuat modificările;
  - c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- 9.6. Se efectuează înregistrarea ieșirii din sistemul automatizat de evidență a salariaților, înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
- a) data și timpul eliberării;
  - b) denumirea informației și căile de acces la aceasta;
  - c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
  - d) ID-ul utilizatorului care a solicitat informația;
  - e) volumul documentului eliberat (numărul paginilor, fișelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.
- 9.7. Cazurile de deranjament al auditului securității în sistemul automatizat de evidență a salariaților sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.
- 9.8. Rezultatele auditului securității în sistemul automatizat de evidență a salariaților (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

## **X. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ SECȚIA RESURSE UMANE**

- 10.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul automatizat de evidență a salariaților, inclusiv instalarea corecțiilor și pachetelor de reînnoire a acestora, protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.
- 10.2. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul automatizat de evidență a salariaților.
- 10.3. Se asigură testarea funcționării corecte a componentelor de securitate a sistemului automatizat de evidență a salariaților (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).
- 10.4. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență a salariaților și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

## **XI. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ SECȚIA RESURSE UMANE**

- 11.1. Persoanele care asigură exploatarea sistemul automatizat de evidență a salariaților trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
- 11.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență a salariaților.
- 11.3. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență a salariaților poartă răspundere civilă, contravențională și penală.

## **XII. DISPOZIȚII FINALE**

- 12.1. Presentul Regulament a fost aprobat de către rectorul Universității de Stat din Moldova la 28.04.2015, cu posibilitatea revizuirii periodice, în funcție de modificările și completările în legislație, precum și de sistemul de evidență.
- 12.2. Modificarea și completarea prezentului Regulament se face în mod stabilit pentru aprobarea lui.
- 12.3. Presentul Regulament se completează cu prevederile legislației în vigoare.