INSTITUŢIA PRIVATĂ DE ÎNVĂŢĂMÂNT SUPERIOR „UNIVERSITATEA AMERICANĂ DIN MOLDOVA”

REGULAMENTUL PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL CONŢINUTE ÎN SISTEMUL DE EVIDENŢĂ RESURSE UMANE

APROBAT
de Senatul Universității
Americane din Moldova
proces verbal nr.3 din 15 decembrie 2020
Președintele Senatului UAM
Dr., hab., prof.univ. AVORNIC Gheorghe

CHIŞINĂU 2020

I. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea datelor cu caracter personal conţinute în sistemul de evidenţă resurse umane (în continuare – Regulament) în cadrul I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA"(în continuare - Universitate), este elaborat în vederea implementării prevederilor Politicii de securitate privind protecţia datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor de evidenţă gestionate de Universitate, a Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor de evidenţă de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum şi întru respectarea art. 91 – 94, Capitolul VI din Codul muncii.

1.2. Prezentul Regulament reglementează condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal ale angajaţilor şi ale potenţialilor angajaţi Universităţii în cadrul sistemului de evidenţă resurse umane

II. SCOPUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1. Prelucrarea datelor cu caracter personal conţinute în sistemul de evidenţă resurse umane are drept scop:

2.1.1. planificarea, organizarea şi monitorizarea procedurilor de personal;

2.1.2. prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii Universităţii şi care au impact asupra raportului de muncă între Universitate şi angajaţii acestuia, precum şi a persoanelor fizice cu care Universitatea intră în relaţii contractuale;

2.1.3. perfectarea contractelor individuale de muncă, ordinelor/dispoziţiilor conducerii, regulamentelor interne ale Universităţii;

2.1.4. prelucrarea ordinelor/dispoziţiilor conducerii referitoare la personal;

2.1.5. furnizarea informaţiei necesare pentru evidenţa contabilă legată de calculele salariale şi rapoartele de muncă în cadrul Universităţii;

2.1.6. prelucrarea manuală a cererilor angajaţilor, emiterea ordinelor/dispoziţiilor privind acordarea primelor, concediilor anuale plătite, concediilor cu menţinerea salariului mediu, deplasărilor de serviciu şi concediilor pe cont propriu ale angajaţilor Universităţii;

2.1.7. eliberarea certificatelor confirmative privind raportul de muncă al angajatului existent în cadrul Universităţii, la cererea angajaţilor în formă scrisă;

2.1.8. prezentarea documentelor aferente evidenţei resurselor umane ce conţin date cu caracter personal către conducerea Universităţii, auditului intern sau extern. În cazul datelor cu caracter personal ale angajaţilor sau ale altor persoane cu care Universitatea se află în relaţie juridică, îi va înştiinţa pe aceşti atunci când datele respective vor fi transmise către terţi;

2.1.9. alte scopuri legale conform cerinţelor legislaţiei muncii în vigoare.

III.CATEGORIILE DE DATE CU CARACTER PERSONAL ALE ANGAJAŢILOR PRELUCRATE ÎN CADRUL SISTEMULUI DE EVIDENŢĂ RESURSE UMANE:

3.1. Numele, prenumele;

3.2. Sexul;

3.3. Data şi locul naşterii;

3.4. Cetăţenia;

3.5. IDNP;

3.6. Imaginea (foto);

3.7. Situaţia familială;
3.8. Situaţia militară;
3.9. Datele personale ale membrilor familiei;
3.10. Situaţia economică şi financiară;
3.11. Datele bancare;
3.12. Semnătura;
3.13. Datele din actele de stare civilă;
3.14. Codul asigurării sociale (CPAS);
3.15. Codul asigurării medicale (CPAM);
3.16. Numărul de telefon/fax;
3.17. Numărul de telefon mobil;
3.18. Adresa (domiciliu/reşedinţa);
3.19. Adresa e-mail;
3.20. Profesia şi/sau locul de muncă;
3.21. Sancţiuni disciplinare;
3.22. Formarea profesională-diplome-studii;
3.23. Obişnuinţe/preferinţe/comportament;
3.24. CV-ul;

3.25. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către Universitate astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/şterge, în funcţie de suportul pe care au fost efectuate. În cazul obligaţiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.
3.26. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidenţă resurse umane în alte scopuri decât cele menţionate mai sus este interzisă.

IV. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

4.1. Datele cu caracter personal conţinute în sistemul de evidenţă resurse umane în cadrul Universităţii se prelucrează/stochează:
1. pe suport de hârtie;
2. în format electronic: măsurile de securitate la prelucrarea datelor în formatul electronic electronic (utilizarea parolelor pentru confirmarea ID-ului utilizatorului):
3. Software – Sistemul de evidenţă resurse umane 1C , versiunea 8.3, care este instalat pe serverul Universităţii şi cu dreptul de acces la computer de către Şeful secţiei Resurse Umane. Computerele se află în blocul administrativ din sediul Universităţii – bd.Ştefan cel Mare şi Sfînt, mun.Chişinău, MD-2001,

4.2. Mentenanţa programului contabil 1C versiune 8.3 este efectuată de către compania Business Logic SRL, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" şi compania Business Logic SRL, cu următoarele atribuţii stabilite companiei prestatoare:
- Efectuarea ajustărilor în program, în baza modificărilor legislaţiei Republicii Moldova;
- Eliminarea erorilor în funcţionarea programului;
- Consultarea în rezolvarea dificultăţilor apărute în utilizarea programului (linia fierbinte);
- Examinarea solicitărilor parvenite din partea Universităţii;
- Examinarea bazei de date a Universităţii (la necesitate);
- Vizite la faţa locului, la solicitarea Universităţii;

- Examinarea şi nedivulgarea informaţiei cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

4.3. Prelucrarea informaţiilor în sistemul de evidenţă resurse umane pe suport de hârtie este structurată după criteriul „mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în blocul administrativ din sediul Universităţii.

V. RESPONSABILITĂŢILE ŞI OBLIGAŢIILE PERSOANEI/PERSOANELOR RESPONSABILE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

5.1. Contractele individuale de muncă, fişele personale ale salariaţilor, registrele, alte formulare care conţin date cu caracter personal se consideră purtători de date cu caracter personal.

5.2. Documentele se păstrează de lucrătorii subdiviziunii Resurse Umane în birouri şi spaţii special amenajate, safeuri care sunt mereu încuiate, acces la acestea o au doar responsabilii.

5.3. Transmiterea datelor personale a salariatului se asigură numai prin personalul subdiviziunii, cu acordul salariatului.

5.4. Nu se permite eliberarea datelor cu caracter personal terţilor neîmputerniciţi.

5.5. În vederea neadmiterii dezvăluirii prin transmitere a datelor cu caracter personal ale angajaţilor, urmează a identifica identitatea persoanelor căror li se eliberează acte ce conţin date cu caracter personal ale angajaţilor.

5.6. Nu se admite furnizarea datelor cu caracter personal ale angajaţilor prin intermediul telefonului.

5.7. Acces în biroul unde se conţin date cu caracter personal ale angajaţilor au doar persoanele împuternicite.

5.8. Datele cu caracter personal ale salariaţilor se utilizează numai în limitele competenţelor funcţionale şi doar în timpul orelor de program.

5.9. Datele cu caracter personal din sistemul de evidenţă resurse umane, la solicitarea subiectului de date şi/sau ale persoanei împuternicite de către acesta (împuternicirile urmează a fi prezentate în modul corespunzător, potrivit legislaţiei în vigoare), pot fi prezentate, rectificate, distruse, cu excepţia cazurilor prevăzute expres de legislaţie.

5.10. Fiecare acces la datele cu caracter personal ale angajaţilor (prezentarea în original a actelor, eliberarea de copii etc.) se consemnează în Registrul de acces.

5.11. Informaţia ce conţine date cu caracter personal nu poate fi extrasă din sistem sau folosită în alte sisteme de evidenţă decât cu consimţământul subiectului de date cu caracter personal sau în situaţiile prevăzute de prevederile art. 5 alin. (5) al Legii privind protecţia datelor cu caracter personal.

5.12. Informaţia ce conţine date cu caracter personal a potenţialilor angajaţi va fi prelucrată pe perioada atingerii scopului, adică – angajarea persoanei, şi cu obţinerea consimţământului scris a potenţialilor angajaţi la prelucrarea datelor cu caracter personal de către serviciul resurse umane (anexa nr. 1).

5.13. În cazul cînd potenţialii angajaţi refuză să semneze consimţământului scris la prelucrarea datelor cu caracter personal, se vor aplica prevederile art. 11 alin. (3) din Legea nr. 133 din 08.07.2011.

VI. ANGAJAŢII SUBDIVIZIUNII RESURSE UMANE NU AU DREPTUL:

6.1. Să obţină şi să prelucreze date referitoare la convingerile politice, religioase, la viaţa privată, apartenenţa salariatului la sindicate, asociaţii obşteşti şi religioase, partide şi alte organizaţii social-politice, date despre viaţa privată a salariatului sau alte date cu caracter personal ale angajaţilor într-un volum ce depăşeşte sau excede limitele legale prevăzute de Legea privind protecţia datelor, Codul muncii etc.

VII. TRANSMITEREA DATELOR PERSONALE ALE SALARIATULUI

7.1. Datele cu caracter personal ale angajaţilor nu pot fi transmise terţilor neîmputerniciţi.
7.2. În cazul în care persoana ce intenţionează colectarea şi prelucrarea unui anumit volum de date cu caracter personal nu întruneşte condiţiile prevederilor art. 4 al Legii privind protecţia datelor cu caracter personal, acesteia i se refuză imediat, şi după caz se înştiinţează organele competente în vederea întreprinderii acţiunilor corespunzătoare.
7.3. Calitatea ierarhică superioară a funcţiei persoanei ce intenţionează să prelucreze datele cu caracter personal ale angajaţilor, nu poate servi drept justificare a ingerinţei în viaţa privată a subiectului de date cu caracter personal/angajat.
7.4. Cererile de acces la datele cu caracter personal ale angajaţilor din partea organelor de forţă, urmează a fi examinate prin prisma prevederilor Codului de procedură penală.
7.5. La transmiterea datelor cu caracter personal ale angajaţilor nu se vor utiliza: e-mail-urile personale, fax, telefonul fix/mobil, şi/sau alte metode care nu oferă un nivel adecvat de protecţie a datelor cu caracter personal.
7.6. La eliberarea oricăror informaţii şi copii de pe documentele oficiale ale angajaţilor, se va include obligatoriu şi marcajul corespunzător din Registrul de evidenţă al operatorilor de date cu caracter personal.

Model: *Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr._____, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal.*

VIII. PĂSTRAREA ŞI MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENŢĂ RESURSE UMANE

8.1. Măsurile generale de administrare a securităţii informaţionale:
8.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic care conţin date preluate din sistemul de evidenţă resurse umane, aceştia se păstrează în safeuri care se încuie.
8.1.2. La finalizarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.
8.1.3. Universitatea asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.
8.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă resurse umane este blocat împotriva vizualizării de către persoane neautorizate.
8.1.5. Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă resurse umane sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a conducătorului Universităţii.
8.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă resurse umane din/în perimetrul de securitate se înregistrează în registru.
8.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă resurse umane, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.
8.3. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă resurse umane, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

8.4. Accesul în biroul unde este amplasat sistemul de evidenţă resurse umane este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

8.5. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.

8.6. Înainte de acordarea accesului fizic la sistemul de evidenţă resurse umane, se verifică competenţele de acces.

8.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

8.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă resurse umane, fiind integru din punct de vedere fizic.

8.9. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde este amplasat sistemul de evidenţă resurse umane, din punct de vedere fizic.

8.10. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

8.11. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

8.12. Amplasarea sistemului de evidenţă resurse umane răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

8.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă resurse umane, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă resurse umane, inclusiv posibilitatea deconectării oricărui component TI.

8.14. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă resurse umane, sunt protejate contra conectărilor nesancţionate sau deteriorărilor.

8.15. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă resurse umane. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

IX. DURATA DE STOCARE

9.1. **Prelucrarea datelor cu caracter personal în sistemul de evidenţă resurse umane se efectuează pe perioada activităţii angajaţilor (din momentul semnării contractului pînă la finalizarea efectuării acţiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).**

9.2. **La expirarea termenelor menţionate în punctul 9.1, datele din sistemul de evidenţă resurse umane sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat de Agenţia Naţională a Arhivelor nr.57 din 27.07.2016.**

X. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

10.1 Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemul de evidenţă resurse umane şi a proceselor executate în numele acestor utilizatori.

10.2 Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

10.3 Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lîngă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

10.4 Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

10.5 Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

10.6 Se asigură, pentru o perioadă de 1 /un/ an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor şi prevenirea folosirii repetate a acestora.

10.7 În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

10.8 Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență resurse umane, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență resurse umane, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 /una/ lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din sistemul de evidență resurse umane. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acțiunii conturilor de acces.

10.9 În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidență resurse umane.

10.10 Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

10.11 Se impun limite în privința persoanelor care au dreptul:

a) să vizualizeze informațiile stocate în sistemul de evidență resurse umane;

b) să copieze, să descarce, să şteargă sau să modifice orice informație stocată.

10.12 Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.

10.13 Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

10.14 Orice încălcare a securității în ceea ce priveşte sistemul de evidență resurse umane este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

10.15 Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemului de evidență resurse umane este controlată şi că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională şi penală.

XI. AUDITUL SECURITĂȚII ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

11.1 Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidenţă resurse umane pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

11.2 Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;

c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

11.3 Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din sistemul de evidenţă resurse umane, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau al procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – pozitivă sau negativă.

7.4. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din sistemul de evidenţă resurse umane, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau a procesului;

c) ID-ul utilizatorului;

d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);

f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

11.4 Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

11.5 Se efectuează înregistrarea ieşirii din sistemul de evidenţă resurse umane, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

a) data şi timpul eliberării;

b) denumirea informaţiei şi căile de acces la aceasta;

c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);

d) ID-ul utilizatorului care a solicitat informaţia;

e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

11.6 Cazurile de deranjament al auditului securităţii în sistemul de evidenţă resurse umane sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

11.7 Rezultatele auditului securităţii în sistemul de evidenţă resurse umane (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

11.8 Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă resurse umane constituie 2 /doi/ ani, în scopul asigurării posibilităţii de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care

investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

XII. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ RESURSE UMANE

12.1 Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă resurse umane, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

12.2 Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din sistemul de evidenţă resurse umane.

12.3 Se asigură testarea funcţionării corecte a componentelor de securitate a sistemului de evidenţă resurse umane (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

12.4 Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă resurse umane şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

XII.GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

13.1 Persoanele care asigură exploatarea sistemului de evidenţă resurse umane trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

13.2 Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă resurse umane.

13.3 „În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar şi să asigure accesul la informaţiile necesare relevante obiectului controlului."

13.4 Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă resurse umane poartă răspundere civilă, contravenţională şi penală.

XIV. RESPONSABILITATEA PENTRU ÎNCĂLCAREA NORMELOR PRIVIND OBŢINEREA, PĂSTRAREA, PRELUCRAREA ŞI STOCAREA DATELOR CU CARACTER PERSONAL

14.1 Prelucrarea datelor cu caracter personal, contrar principiilor de protecţie a datelor cu caracter personal, duce la răspunderea civilă, contravenţională şi după caz penală.

XV. DISPOZIŢII FINALE

15.1 Prezentul Regulament este adus la cunoştinţa angajaţilor Universităţii, contra semnătură.

15.2 Prezentul Regulament, la necesitate, este revizuit, modificat, completat şi este aprobat prin ordinul conducătorului Universităţii.

15.3 Orice modificare efectuată este adusă la cunoştinţa angajaţilor din cadrul Universităţii, contra semnătură.