



**INSTITUȚIA PRIVATĂ DE ÎNVĂȚĂMÎNT SUPERIOR  
„UNIVERSITATEA AMERICANĂ DIN MOLDOVA”**

**REGULAMENTUL  
registrului de evidență a corespondenței al  
I.P.Î.S. ”UNIVERSITATEA AMERICANĂ DIN MOLDOVA”**

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



**CHIȘINĂU 2020**

## I. Dispoziții generale

1. Regulamentul Registrului de evidență a corespondenței al I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" (Regulamentul) este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19 iulie 2018, Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995, Regulilor de întocmire a documentelor organizatorice și de dispoziție și Instrucțiunii-tip cu privire la ținerea lucrărilor de secretariat în organele administrației publice centrale de specialitate și ale autoadministrării locale ale Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 618 din 05 octombrie 1993, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.

2. Prezentul Regulament reglementează modalitatea ținerii Registrului de evidență a corespondenței al I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", precum și procedura de înregistrare, securizare, modificare și radiere a datelor din acest Registru.

3. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută de Legea cu privire la registre, Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19 iulie 2018, Legea privind protecția datelor cu caracter personal, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

Astfel, în sensul prezentului Regulament se definesc următoarele noțiuni:

*Petiție* – orice cerere, sesizare sau propunere adresată unei autorități publice de către o persoană fizică sau juridică;

*Cerere* – orice cerere prin intermediul căreia se solicită emiterea unui act administrativ individual sau efectuarea unei operațiuni administrative;

*Sesizare* – orice sesizare prin intermediul căreia se informează autoritatea publică cu privire la o problemă de interes personal sau public;

*Propunere* – orice propune prin intermediul căreia se urmărește realizarea de către autoritatea publică a unor acțiuni de interes public;

*Registrul de evidență a corespondenței* – resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată și manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia constă în asigurarea evidenței corespondenței parvenite la I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA";

*Registrator* – angajatul I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" împuternicit cu atribuțiile de introducere, modificare, păstrare a informației din Registru.

*Furnizorul datelor* - persoana fizică sau reprezentantul persoanei juridice de drept public sau privat, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

4. Subiecți ai raporturilor juridice apărute ca rezultat al instituirii, administrării și ținerii manuale a Registrului sînt:

- I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", în calitate de proprietar și deținător al Registrului;
- Persoanele împuternicite de ținerea Registrului și cele responsabile de efectuarea controlului intern al ultimului;
- Persoanele fizice, ale căror date cu caracter personal vor fi stocate în Registru;
- Persoanele interesate de a accesa și vizualiza datele din Registru.

5. Angajații I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" poartă răspundere personală pentru îndeplinirea cerințelor prezentului Regulament, asigurarea confidențialității, securității și păstrarea în stare corespunzătoare a informației din Registru.

## II. Condiții generale față de ținerea Registrului

6. Registrul de evidență a corespondenței reprezintă un sistem mixt ce utilizează atât evidența în formă electronică, cât și în formă manuală.

7. De către Direcția corespondență va fi asigurată ținerea în formă manuală a unor componente al Registrului (ținând cont de competența funcțională) prin înscrierea informației, inclusiv păstrarea cărții Registrului de către un angajat împuternicit în acest sens (registratorul) din cadrul subdiviziunii respective, în conformitate cu prevederile legislației în vigoare.

8. Persoanele responsabile din cadrul (DENUMIREA SUBDIVIZIUNII) vor asigura suplimentar evidența în formă electronică a corespondenței parvenite la I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

9. Obiectul înregistrării reprezintă informația referitor la persoanele care au depus adresări în adresa I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

10. Registrul va fi ținut în limba de stat.

11. Registratorul este obligat:

- să introducă în Registru numai informație veridică, colectată de la adresant sau din alte surse neinterzise de lege;
- să asigure evidența în ordine cronologică a fiecărei înscrieri în Registru;
- să nu admită modificarea neîntemeiată a datelor introduse în Registru;
- să efectueze înregistrările în Registru astfel, încât să excludă posibilitatea de a fi radiată (ștearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);
- să asigure accesul la informația din registru doar persoanelor care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare;
- să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

12. Datele din registru vor reflecta starea veridică și actuală a informației privind persoanele vizate în corespondența al I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

13. Atât forma manuală, cât și cea electronică a Registrului va cuprinde în mod obligatoriu:

- denumirea Registrului;
- denumirea I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" ca proprietar, posesor și deținător al Registrului;
- numele, prenumele și funcția persoanei responsabile de introducerea datelor în Registru și a administratorului acestuia;
- numele, prenumele și funcția persoanei care va exercita controlul asupra ținerii Registrului;
- numărul Registrului, termenele de ținere și păstrare a acestuia.

14. Datele cu caracter personal din Registru vor fi prelucrate în condițiile stabilite de legislația privind protecția datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor registrului și de protecție a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acțiuni ilegale la ținerea registrului.

## III. Condiții generale privind introducerea informației în Registru

15. Informația privind corespondența parvenită în adresa I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" va fi recepționată și înregistrată în aceeași zi de persoana responsabilă din cadrul Direcției corespondență în Registrul de evidență a corespondenței și după caz, în fișele de evidență și control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică a I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

16. Înregistrarea informației în Registru se face prin introducerea mențiunilor necesare în cartea de înregistrări (forma manuală) și în Sistemul informatic Microsift Excel (forma electronică) în baza

datelor furnizate prin documentele transmise atât de furnizorul datelor registrului, atât pe suport de hârtie sau în formă electronică, perfectate în modul stabilit de lege.

17. La înregistrarea corespondenței, pe prima pagină se va aplica ștampila de înregistrare în care se indică data primirii și indicele de înregistrare. Indicele de înregistrare constă după caz, din litera inițială a numelui și prenumelui adresantului, numărul și anul de înregistrare a înscrisului.

18. După caz, se va întocmi manual fișa de evidență și control pentru fiecare adresare (în condițiile stabilite prin Instrucțiunile privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995), introducându-se datele cu caracter personal ce vizează petiționarul (nume, prenume, adresa de domiciliu, numărul de telefon) precum și rezoluția conducerii I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", termenul de soluționare stabilit de conducerea I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", datele despre starea executării etc.

19. După examinarea și soluționarea definitivă, pe fișa de evidență și control se aplică semnătura persoanei responsabile de evidență, iar în Sistemul informatic Microsift Excel se face mențiunea despre finalizarea acesteia și modificarea statutului ca arhivată.

20. Modificările și radierile făcute în Registru se efectuează în baza deciziei și cu semnătura registratorului în situația existenței unui motiv întemeiat în acest sens.

21. Dacă furnizorul datelor registrului se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul va face, în modul stabilit, corectările necesare și va informa despre aceasta furnizorul datelor.

22. Greșelile de ordin tehnic comise de către persoana împuternicită de ținerea Registrului se rectifică de către aceasta. Corectarea greșelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

23. Radierea obiectului din Registru se face prin inserarea unei note speciale (care trebuie să conțină semnăturile persoanei responsabile și data radierii) și nu reprezintă excluderea fizică a datelor despre obiect din Registru.

24. Rectificările și radierile înscrisurilor din Registru se efectuează astfel încât textul inițial să fie citabil.

#### **IV. Condiții generale privind păstrarea și furnizarea informației din Registru**

25. Păstrarea Registrului este asigurată de registrator pînă la adoptarea deciziei conducerii I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" despre lichidarea registrului, dar nu mai mult decît pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

26. Ținerea Registrului este supusă controlului intern și extern, în conformitate cu prevederile art. 31 al Legii cu privire la registre.

27. În acest sens, persoana împuternicită de ținerea și păstrarea Registrului este obligată:

- să prevină accesul nesancționat la datele stocate în Registru;
- să întreprindă acțiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informației conținute în acesta, de modificare sau nimicire a acestor date.

28. Persoanele împuternicite de ținerea și controlul registrului sînt obligate să nu divulge informația la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității în cadrul I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

29. Registratorul este obligat să asigure accesul la informația din registru pentru angajații autorizați ai I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" și alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul și interesul legitim de a primi aceste informații, din momentul în care acestea vor fi disponibile, dar nu mai tîrziu de 5 zile lucrătoare de la data depunerii cererii.

30. Informația poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informație.

31. Extrasul din Registrul trebuie să fie semnat de conducerea I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", cu indicarea datei întocmirii/eliberării acestuia.

#### **V. Condițiile suplimentare privind gestionarea Registrului în forma manuală**

32. Ținerea manuală a Registrului de evidență a corespondenței se efectuează sub formă de fișier sau prin introducerea mențiunilor în cartea pentru înregistrări.

33. În acest sens, evidența corespondenței în cadrul I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" este dusă prin intermediul mai multor Registre ținute în formă manuală, cum ar fi:

- „Registrul de intrare și ieșire a petițiilor adresate I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA", gestionate de persoana desemnată din cadrul Direcției corespondență
- „Registrul de intrare/ieșire a corespondenței”, gestionat de persoana desemnată din cadrul Direcției corespondență;
- „Registrul de intrare/ieșire a corespondenței”, gestionat de persoana desemnată din cadrul Direcției corespondență;

34. Registratorul, suplimentar la cele expuse în Cap. IV, în cazul gestionării Registrului în formă manuală, este obligat:

- să efectueze înscrierile citeț și clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greșit se taie cu o linie, fiind posibilă citirea textului greșit înscris.
- să nu înlocuiască neîntemeiat filele din cartea registrului prin extragerea lor, încluirea unor noi file etc;
- să asigure, în cazul deteriorării cărții, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informației, ce se conține în ea;
- să asigure șnuruirea cărților pentru înregistrări (în caz că nu este o carte integrală) și numerotarea filelor. Numărul de file se indică pe ultima pagină și se autentifică (inclusiv conținutul cărții) prin aplicarea semnelor de control de către conducerea I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA": semnătura și ștampila.

35. Informația va fi introdusă în Registrul în ordine cronologică, ținându-se cont de necesitatea prezenței mențiunilor privind:

- numărul de ordine a mențiunii;
- numărul și data de intrare;
- numele și prenumele;
- conținutul succint al documentului;
- numele și prenumele executantului, termenul de executare și rezoluția conducerii I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA";
- rezultatul examinării: admisă/respinsă/oferte explicații de rigoare/acte de reacționare adoptate de conducerea I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

36. Registrul se păstrează de persoana responsabilă într-un safeu metalic și va conține un compartiment separat în care se vor consemna înregistrările de audit a securității, prevăzute de pct. 93 al Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

#### **VI. Condiții suplimentare privind gestionarea Registrului în formă electronică**

37. Ținerea în formă electronică a Registrului de evidență a corespondenței este realizat de I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" prin intermediul unui sistem informațional automatizat special constituit - Sistemul informatic Microsift Excel.

38. Introducerea, modificarea și păstrarea informației în acest Registrul este asigurată de

registratorul desemnat din cadrul Direcției corespondență .

39. La înscrierea informației privind corespondența parvenită, în Registrul se inserează și o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, și anume:

- tipul adresării;
- data și numărul de intrare;
- termenul de rezolvare și data expirării;
- numele, prenumele adresantului;
- adresa de domiciliu, e-mail (în cazul existenței);
- numărul de telefon fix/mobil;
- conținutul succint al adresării;
- rezoluția conducerii I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA";
- persoana responsabilă de control și executorul;
- copia scanată, în format „.pdf” a adresării;
- date privind executarea;
- date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea adresantului;
- rezultatul examinării: admisă/respinsă/oferite explicații de rigoare/acte de reacționare adoptate de I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA".

#### **VII. Măsurile de protecție a datelor cu caracter personal prelucrate în registrul de evidență a corespondenței**

40. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din registrul de evidență a corespondenței, aceștia se păstrează în safeuri care se încuie.

41. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.

42. Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.

43. Accesul fizic la mijloacele de reprezentare a informației preluate din registrul de evidență a corespondenței este blocat împotriva vizualizării de către persoane neautorizate.

44. Mijloacele de prelucrare a informațiilor preluate din registrul de evidență a corespondenței sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

45. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din registrul de evidență a corespondenței din/în perimetrul de securitate se înregistrează într-un registru specializat.

46. Măsurile de protecție a datelor cu caracter personal, prelucrate în registrul de evidență a corespondenței, se înfăptuiesc ținînd cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

47. Cerințe speciale față de marcare: toate informațiile ieșite din registrul de evidență a corespondenței, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

*Model Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. \_\_\_\_\_, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal [www.registru.datepersonale.md](http://www.registru.datepersonale.md). Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal*

48. Accesul în biroul unde este amplasat registrul de evidență a corespondenței este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și/sau cheia de la lacătul mecanic.

49. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.

50. Înainte de acordarea accesului fizic la registrul de evidență a corespondenței, se verifică competențele de acces.

51. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă, conform cerințelor prevăzute în instrucțiunile cu privire la ținerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat registrul de evidență a corespondenței, fiind integru din punct de vedere fizic.

53. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat registrul de evidență a corespondenței, din punct de vedere fizic.

54. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

55. Ușile și ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

56. Amplasarea registrului de evidență a corespondenței răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității registrului de evidență a corespondenței, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la registrul de evidență a corespondenței, inclusiv posibilitatea deconectării oricărui component TI.

58. Computerele, unde este amplasat fizic registrul de evidență a corespondenței, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

59. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din registrul de evidență a corespondenței, sînt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaționale.

60. Securitatea antiincendiară a registrului de evidență a corespondenței: biroul unde este amplasat registrul de evidență a corespondenței este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiară în vigoare.

61. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul registrului de evidență a corespondenței. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

### **VIII Identificarea și autentificarea utilizatorului registrul de evidență a corespondenței**

62. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din registrul de evidență a corespondenței și a proceselor executate în numele acestor utilizatori.

63. Toți utilizatorii (inclusiv administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnamentele nivelului de accesibilitate al utilizatorului.

64. 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.

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

66. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor 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, în mod automatizat.

67. Se 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.

68. 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 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 și autentificare se revocă sau se suspendă.

69. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în registrul de evidență a corespondenței, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în registrul de evidență a corespondenței, 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 registrul de evidență a corespondenței. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

70. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieste cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la registrul de evidență a corespondenței.

71. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

72. Se impun limite în privința persoanelor care au dreptul:

73. să vizualizeze informațiile stocate în registrul de evidență a corespondenței;

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

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

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

77. Orice încălcare a securității în ceea ce privește registrul de evidență a corespondenței este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

78. Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea registrului de evidență a corespondenței este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

## IX. Auditul securității în sistemele de evidență a documentelor

79. Se organizează generarea înregistrărilor de audit a securității în registrul de evidență a corespondenței pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

80. 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.

81. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din registrul de evidență a corespondenței, 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.

82. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din registrul de evidență a corespondenței, 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.

83. 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.

84. Se efectuează înregistrarea ieșirii din registrul de evidență a corespondenței, 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, filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

85. Cazurile de deranjament al auditului securității în registrul de evidență a corespondenței 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.

86. Rezultatele auditului securității în registrul de evidență a corespondenței (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.

87. Durata minimă a stocării rezultatelor auditului securității în registrul de evidență a corespondenței constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

## **X. Asigurarea integrității informațiilor din registrul de evidență a corespondenței**

88. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din registrul de evidență a corespondenței, 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.

89. 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 a registrul de evidență a corespondenței.

90. Se asigură testarea funcționării corecte a componentelor de securitate a registrul de evidență a corespondenței (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

91. 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 registrul de evidență a corespondenței 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 registrul de evidență a corespondenței**

92. Persoanele care asigură exploatarea registrul de evidență a corespondenței 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.

93. 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 registrul de evidență a corespondenței.

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

95. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din registrul de evidență a corespondenței poartă răspundere civilă, contravențională și penală.

## **XII. Dispoziții finale**

96. Prezentul Regulament este revizuit și ulterior aprobat de către administratorul I.P.Î.S. "UNIVERSITATEA AMERICANĂ DIN MOLDOVA" periodic, însă cel puțin o dată în an, precum și la necesitate.

97. Prezentul Regulament se completează cu prevederile legislației în vigoare.

98. Regulamentul este adus la cunoștința angajaților contra semnăturii.

99. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.