APROB
Rector UnAŞM
Maria Duca
26 2015

POLITICA
de asigurare a securităţii datelor cu caracter personal în cadrul Universităţii Academiei de Ştiinţe a Moldovei

I.DISPOZIŢII GENERALE

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal au drept scop stabilirea regulilor de implimentare de către **Universitatea Academiei de Ştiinţe a Moldovei** (în continuare UnAŞM) a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidentialităţii şi integrităţii datelor cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi mecanice de date cu caracter personal şi/sau registrelor ţinute manual, în conformitate cu prevederile Legii RM nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal şi Hotărîrii Guvernului RM nr.1123 din 14.12.2010 privind Cerinţele faţă de asigurarea securităţii datelor cu caracter personal.

II. CERINŢE GENERALE

1. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemului informaţional de date cu caracter personal şi vor fi efectuate neîntrerupt de către persoanele responsabile, angajate la UnAŞM.

2. Protecţia datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

3. Sunt supuse protecţiei toate resursele informaţionale ale UnAŞM, care conţin date cu caracter personal inclusiv :
   a) suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
   b) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi spaţiu multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei;
   c) carnetele de muncă, dosarele personale ce conţin acte ale persoanelor, suporturi de hârtie etc.

4. Protecţia datelor cu caracter personal este asigurată în scopul:
   a) preîntmpânării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
   b) respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
   c) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal;
   d) recunoaşterii şi respectării dreptului la viaţă intimă, familială şi privată, prelucrarea datelor cu caracter personal desfăşurandu-se în conformitate cu prevederile legale în vigoare.

III. POLITICA DE SECURITATE A DATELOR CU CARCTER PERSONAL

5. Prin Ordinul UnAŞM este nominalzată persoana responsabilă de întocmirea, menţinerea, modificarea şi actualizarea politicii de securitate a UnAŞM.

6. Măsurile de securitate sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal. La UnAŞM sunt create **5 sisteme informaţionale:**
   - Secţia Resuse umane;
   - Secţia Studii şi managementul calităţii;
   - Secţia Şcoli doctorale şi instruire continuă;
   - Secţia Contabilitate şi finanţe;
   - Sistemul informaţional(reţeua de calculatoare).

7. Mecanismul de punere în aplicare a măsurilor de securitate este prevăzut de prezenta Politică de Securitate, prin Regulamentele interne privind prelucrarea şi asigurarea securităţii informaţiilor ce conţin date cu caracter personal ale celor 5 subdiviziuni şi Nomenclatorul datelor cu caracter personal ,prelucrate în cadrul UnAŞM.

8. Lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal este stabilită prin ordinul intern al UnAŞM.

9. Documentaţia tehnică cu privire la controalele de securitate este ţinută sub formă de registru de către persoana responsabilă, numită prin ordinul UnAŞM pentru fiecare sistem informaţional în parte.

10. Orarul controalelor de securitate este stabilit de către persoana numită responsabilă, în conformitate cu regulamentul de securitate al fiecărui sistem care prelucrează date cu caracter personal.

11. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoştinţa conducerii Universităţii în mod de urgenţă, pentru a putea fi identificată procedura de soluţionare a incidentului.

IV. SECURITATEA MEDIULUI FIZIC ŞI A TENOLOGIILOR INFORMAŢIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Secţiunea 1

12. Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care îndeplinesc funcţiile stipulate în Regulamentele interne privind prelucrarea şi asigurarea securităţii informaţiilor ce conţin date cu caracter personal ale celor 5 subdiviziuni şi doar în timpul orelor de program şi însemnelor corespunzătoare (ecusoane).
Acesul în camera de servere este permisă doar personalului IT, administratorului care este numit prin ordin. Personalul străin are acces în această încăpere doar sub stricta supraveghere a uni specialist IT. Toate operaţiunile de acces la servere sau alte mijloace tehnice sau software se fac de către personalul IT al UnAŞM.

Secţiunea 2

13. **Administrarea şi monitorizarea accesului fizic.**Se efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal,inclusive se reacţionează ca încălcarea regimului de acces.

14. **Camera de servere** este echipată cu uşă metalică şi gratii metalice la ferestre.

15. Perimetrul sediilor şi încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu carcter personal sunt păstrate integri din punct de vedere fizic, toţi pereţii sunt întregi, uşile se încuie, iar ferstrele se închid.

16. Pereţii exterior ai încăperilor sînt rezistenţi, întrările echipate cu lacăte. Birourile amplasate la parter au au ferestrele echipate cu gratii. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii.

17. Înainte de acordarea accesului fizic la sistemele informaţionale de date cu carcter personal se verifică **competentele de acces**. Persoanele noi angajate sunt instruite în domeniul prelucrării datelor cu carcter personal şi semnează declaraţia de confidenţialitate emisă în acest sens.

18. Toate fişele personale ale fiecărui angajat, inclusiv carnetele de muncă, sunt păstrate în safeu metallic fiind ocrotit împotriva incendiilor ,în secţia resurse umane a UnAŞM.

19. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

20. Folosirea tenhicii foto,video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii deţinătorului de date cu caracter personal

Secţiunea 3

21. Persoanele care accesează sediile UnAŞM sunt **supravegheate de camerele video** . În birourile cu acces interzis pot întra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceştia vor fi rugaţi să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoştinţa conducerii UnAŞM.

Secţiunea 4

22. Se asigură **securitatea echipamentului electric** utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia cele comunicaţionale pentru a exclude bruiajul. Specialiştii IT a UnAŞM efectuează controale, acestora contra deteriorării şi conectărilor nesancţionate. Cablurile de tensiune sunt separate de nu mai rar decât o dată în lunăr în scopul verificării cazurilor de conectare neautorizate la cablurile de reţea.

Secţiunea 5

23. UnAŞM dispune de mijloace de asigurare a securităţii antiincendiare a sediilor /oficiilor/ birourilor unde sunt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Secţiunea 6

24. Pentru asigurarea securităţii informaţionale în cazul neutilizării temporare a purtătorilor **de** informaţie pe suport de hârtie sau electronică (digitală) care conţin date cu caracter personal, aceştea se păstrează în safeuri sau dulapuri metalice care se încuie. Computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi cele de copiere. Accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis şi controlat. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Rectorului UnAŞM .

V. IDENTIFICAREA ŞI AUTETIFICAREA UTILIZATOTULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

Secţiunea 1

25. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt folosite parole. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă în mod automat în decursul a două săptămînă de la ultimul acces sau în mod individual imediat, la momentul introducerii modificării în raportul de muncă.

26. Se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor ce includ:

a) păstrarea confidenţialităţii parole;
b) interzicerea înscrierii parole pe suport de hârtie, în cazul în care nu se asigură securitatea păstrăriiacestora;

c) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului;
d) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;
e) modificarea parolelor peste intervale de maximum 3 luni;
f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate.

27. Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinaţie complexă. În mod obligatoriu fiecare parolă conţine una sau mai multe litere scrise cu majuscule (sa fie tot cu litera mare). Parola nu va conţine iniţialele sau date care pot caracteriza o anumită persoană (data de naştere, adresa, poreclă,etc.)

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Secţiunea 1

28. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

Secţiunea 2

29. **Drepturile de acces ale utilizatorilor** la sistemele informaţionale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni)şi după oricare schimbare de statut al utilizatorului.

Secţiunea 3

30. **Repartizarea obligaţiilor** subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin ordinul UnAŞM . Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competente,care sunt necesare pentru realizarea de către ei a obiectivelor stabilite .

31. Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal,se blochează (la solicitarea utilizatorului sau automat, după maximum 15 minute de perioadă inactivă a utilizatorului), fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

Secţiunea 4

32. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal trebuie securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum şi sunt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Secţiunea 5

33. Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării şi controlului şi este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei. Folosirea tehnologiilor fără fir se autorizează de personalul IT al UnaŞAM.

Secţiunea 6

34. Se stabilesc limitări şi se elaborează reguli de folosire a echipamentului portativ şi mobil care permit accesul la sistemele informaţionale de date cu caracter personal. Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil se documentează, fiind monitorizat şi controlat. Folosirea echipamentului portativ şi mobil este autorizată de Serviciul Tehnologii Informaţionale al UnAŞM.

VII. PROTECŢIA SISTEMELOR INFORMAŢIONALE ŞI A COMUNICAŢIILOR ÎN CARE SUNT PRELUCRATE DATE CU CARACTER PERSONAL

Secţiunea I

35. Se asigură izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.
Trebuie preîntâmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile .

Secţiunea 2

36. Se asigură protecţia sistemelor informaţionale de date cu caracter personal sau sunt limitate posibilităţile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) - „refuz în serviciu".

37. Se efectuează monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale. Amplasarea resurselor general accesibile se asigură în spaţiile special destinate a reţelei de calcul cu interfeţele fizice de reţea. Este asigurată imposibilitatea accesului din exterior al utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

38. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal se asigură confidenţialitatea datelor cu caracter personal transmise, utilizându-se mijloace de protecţie criptografică a informaţiei.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

39. Responsabilul fiecărui sistem informaţional este obligat să întocmească următoarele proceduri obligatorii de audit al sistemului :

1) Se efectuiează 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 negative.

2) Este efectuată înregistrarea tentativelor de pornire/finisare a sesiunii de lucru a programelor aplicative şi a proceselor, destinate prelucrării datelor cu caracter personal, 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.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau 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 negative.

4) Este efectuată înregistrarea modificărilor drepturilor de acces ale 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.

5) Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), 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, a filelor, copiilor) şi rezultatul eliberării.

40. În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

41. Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul.

42. Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

43. Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

Secţiunea 1

44. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

Secţiunea 2

45. Se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv a altora care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

Secţiunea 3

46. Se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi a informaţiei care conţine date cu caracter personal.

Secţiunea 4

47. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat, la pornirea sistemului, şi lunar, la solicitarea utilizatorului autorizat în acest scop).

X. COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Secţiunea 1

48. Reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către deţinătorul de date cu caracter personal intervalul de timp în care se execută copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urile folosite pentru prelucrarea automatizată a datelor cu caracter personal, dar în orice caz acest termen este mai mic de un an, care se păstrează în locuri protejate, în afara zonei de amplasare a acestei informaţii şi soft-urile de bază.

Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal.

Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

XI. CONTROALELE DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Secţiunea 1

49. Deţinătorii de date cu caracter personal verifică cu regularitate, cel puţin o dată pe an, îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu character personal asistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necessitate.

50. Controalele de securitate sunt actualizate de fiecare dată cînd deţinătorul de date cu caracter personal este reorganizat sau îşi schimbă infrastructura.

Secţiunea 2

51. În scopul verificării nivelului de protecţie a sistemelor informaţionale de date cu caracter personal, precum şi în scopul preîntîmpinării unor eventuale cazuri de acces ilicit sau întîmplător asupra acestor sisteme informaţionale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaţionale de date cu caracter personal.

Secţiunea 3

52. Rezultatele controalelor efectuate de Centru sunt puse imediat la dispoziţia deţinătorului de date cu caracter personal, nivelul de protecţie a sistemelor informaţionale de date cu caracter personal a căruia a servit obiect al controlului, cu prescrierea, în caz de necesitate, a acţiunilor necesare de a fi întreprinse în vederea asigurării securităţii prelucrării datelor cu caracter personal