APROBAT
Senatul USMF„Nicolae Testemițanu”
Proces-verbal nr. 3 din 14 mai 2015

POLITICA
de securitate a prelucrării datelor cu caracter personal în cadrul Universității de Stat de Medicină și Farmacie „Nicolae Testemițanu”

I. DISPOZIŢII GENERALE

1. Politica de securitate a prelucrării datelor cu caracter personal în cadrul Universității de Stat de Medicină și Farmacie „Nicolae Testemițanu” (în continuare – Politica) stabilește principiile și cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale automatizate şi mecanice de date cu caracter personal.

2. Politica are drept scop stabilirea regulilor de implementare de către Universitatea de Stat de Medicină și Farmacie „Nicolae Testemițanu” (în continuare - Universitate) a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale automatizate şi mecanice de date cu caracter personal şi/sau registrelor ţinute manual.

3. Politica este elaborată în conformitate cu prevederile Legii Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal şi Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Hotărîrii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, precum şi Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (Strasbourg, 28 ianuarie 1981).

4. În sensul prezentei Politici, se definesc următoarele noţiuni:

autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

fişiere temporare - ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate - certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

politica de securitate a datelor cu caracter personal - document, elaborat de către Universitate, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sînt expuse acestea;

perimetru de securitate - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei, care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

protecţia informaţiei contra acţiunilor neintenţionate - ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

purtător de date cu caracter personal - suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;

restaurarea datelor - procedurile cu privire la reconstituirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

tehnologie informaţională (TI) - totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

utilizator - persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

sesiune de lucru - perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi pînă la momentul opririi acestora;

sistem informaţional de date cu caracter personal - totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caràcter personal;

stocare - păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINŢE GENERALE

5. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemelor informaţionale de date cu caracter personal şi vor fi efectuate neîntrerupt de către persoanele responsabile angajate la Universitate.

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

7. Orice prelucrare a datelor cu caracter personal, cu excepţia prelucrării lor strict menţionate în Legea nr. 133 din 08.07.2001 privind protecţia datelor cu caracter personal, poate fi

efectuată numai dacă persoana vizată şi-a dat consimțământul în mod expres şi neechivoc pentru acea prelucrare.

8. Persoanele angajate în câmpul muncii sau admise la diverse forme de instruire vor fi informate în scris despre prelucrarea datelor cu caracter personal conform Legii nr. 133 din 08.07.2001 privind protecţia datelor cu caracter personal.

9. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale şi mecanice de date cu caracter personal ale Universității se realizează ţinîndu-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.

10. Sunt supuse protecţiei toate resursele informaţionale ale Universității, 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 multiplicare a documentelor şi alte mijloace de prelucrare a informaţiei.

11. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:
    a) preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
    b) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
    c) respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
    d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
    e) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

12. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:
    a) preîntîmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
    b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
    c) preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
    d) preîntîmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care

condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.

13. Preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.

14. Preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă.

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

15. Prin ordinul Rectorului este nominalizat responsabilul de implementarea în practică şi actualizarea prezentei Politici (prorector).

16. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem informaţional care prelucrează date cu caracter personal.

17. Responsabilul de administrarea fiecărui sistem informaţional se stabileşte prin ordinul Rectorului, iar mecanismul de punere în aplicare a măsurilor de securitate este prevăzut de prezenta Politică.

18. Nomenclatorul datelor cu caracter personal prelucrate în cadrul Universităţii este stabilit de Regulamentul de securitate al fiecărui sistem, care prelucrează date cu caracter personal.

19. Categoriile de utilizatori autorizaţi să acceseze datele cu caracter personal sunt stabilite prin ordinul Rectorului.

20. Configurarea sistemului informaţional de date cu caracter personal şi a reţelei are loc în conformitate cu cerinţele tehnice stabilite prin Sistemul de management al securităţii informaţionale (SMSI), aprobat prin ordinul Rectorului.

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

22. 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.

23. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanelele împuternicite prin ordinul Rectorului.

IV. SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAŢIONALE UTILIZATE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

24. Autorizarea accesului fizic

24.1 Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (permis nominal de acces), conform listei nominale de acces la sistemul informaţional.

24.2 Drept excepţie, în sediul Universității este permis accesul persoanelor fizice străine în mod obligatoriu sub monitorizarea de către personalul Universității pe perioada aflării lor în birou, pentru a exclude careva acces la sistemele informaţionale.

24.3 Accesul în camera de servere este permisă doar personalului Departamentului Tehnologia Informației și Comunicațiilor (în continuare - TIC), personalul străin având acces în această încăpere doar sub stricta supraveghere a unui specialist TIC, iar toate operaţiunile de acces la servere sau alte mijloace tehnice se fac de către şeful TIC sau persoana autorizată cu înregistrările respective.

24.4 Administrarea şi monitorizarea accesului fizic se efectuează în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.

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

24.6 Toate carnetele de muncă sunt păstrate în safeu metalic, protejat împotriva incendiilor.

25. Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal:

25.1 Perimetrul sediilor şi încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate integre din punct de vedere fizic, toţi pereţii sunt întregi, uşile se încuie, iar ferestrele se închid.

25.2 Pereţii exteriori ai încăperilor sunt rezistenţi, intrările echipate cu lacăte.

25.3 Computerele, serverele şi alte terminale de acces, în limita posibilităţii sunt amplasate în locuri cu acces limitat pentru persoane străine.

25.4 Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii. Ca măsură suplimentară sporită pentru securitatea datelor cu caracter personal, birourile Departamentului Resurse Umane și Departamentul Evidență și Gestiune Contabilă, sunt date la servicii de pază.

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

26. Folosirea tehnicii 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.

27. Controlul vizitatorilor este supravegheaţi în încăperile unde aceştia au acces, în birourile cu acces interzis aceştia pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceşti vor fi rugaţi să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoştinţa administrației imediat.

28. Securitatea electroenergetică asigură integritatea funcţională a echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate.

28.1 În cazul situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

28.2 Universitatea dispune de surse autonome de alimentare cu energie electrică de scurtă durată, care sînt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

29. Securitatea cablurilor de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, asigură protejarea contra conectărilor nesancţionate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaţionale pentru a exclude bruiajul. Specialiştii TIC efectuează controale, nu mai rar decât o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

30. Universitatea 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.

31. Controlul instalării şi scoaterii componentelor TI asigură evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal. Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

32. Măsurile generale de administrare a securităţii informaţionale se realizează în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia fiind păstraţi 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 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 mijloacele de program destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Rectorului.

V. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

33. Identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori este obligatorie. Toţi utilizatorii (inclusiv personalul care asigură susţinerea 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.

    33.1 Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. În cazul în care contractul individual de muncă 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 săptămîni de la ultimul acces, sau în mod individual imediat la momentul introducerii modificării în raportul de muncă.

    33.2 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 majusculă. Parola nu va conţine iniţialele sau date care pot caracteriza o anumită persoană (data de naştere, adresă, poreclă, etc.).

34. Identificarea şi autentificarea echipamentului este asigurată prin posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal.

35. Administrarea identificatorilor utilizatorilor include:
    a) identificarea univocă a fiecărui utilizator;
    b) verificarea autenticităţii fiecărui utilizator;
    c) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declaraţiei de confidenţialitate şi trecerii procedurii de instruire;
    d) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
    e) dezactivarea contului de utilizator după o perioadă inactivă;
    f) executarea copiilor de arhivă a ID-urilor utilizatorilor.

36. Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor se asigură prin conexiunea bilaterală a Universităţii cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

37. Utilizarea parolelor în procesul asigurării securităţii informaţionale respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:
    a) păstrarea confidenţialităţii parolelor;
    b) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;
    c) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
    d) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt 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 anumite intervale de timp (cel putin 6 luni) şi la necesitate;
    f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

38. Administrarea parolelor utilizatorilor utilizează identificatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. Se asigură blocarea accesului după trei tentative greşite de autentificare. Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o

perioada de un an) şi prevenirea folosirii repetate a acestora. La momentul introducerii, parolele nu se reflectă în clar pe monitor. Parolele se păstrează în formă cifrată, utilizîndu-se algoritmul criptografic unilateral (funcţia hash).

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

39. Administrarea accesului se implementează prin mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

40. Administrarea conturilor de acces (account-urilor) este efectuată prin administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

41. Acordarea accesului la sistemele informaţionale de date cu caracter personal este autorizat în conformitate cu prezenta Politică.

42. Revizuirea drepturilor de acces ale utilizatorilor sunt 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.

43. 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 Rectorului întocmit în acest sens. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

44. Înainte de acordarea accesului în sistem, utilizatorii sînt 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.

45. Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 5 minute de perioadă inactivă a utilizatorului fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

46. Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

47. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sînt securizate (utilizîndu-se VPN, criptarea, cifrarea etc), precum şi sînt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de Universitate şi este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

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

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

49. Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

50. Se asigură izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.

51. Sunt preîntîmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile.

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

53. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sînt prelucrate date cu caracter personal.

54. 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. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

55. Se asigură confidenţialitatea datelor cu caracter personal transmise, utilizîndu-se mijloace de protecţie criptografică a informaţiei.

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

56. Înregistrările de audit a securităţii registrelor ţinute manual în care sînt prelucrate date cu caracter personal, trebuie să conţină: numele şi prenumele utilizatorului; numele fişei accesate (pagina şi inscripţia din registru); numărul înregistrărilor efectuate; tipul de acces; data accesului (an, lună, zi); timpul (ora, minuta) şi durata accesului.

57. Responsabilul de administrarea sistemelor informaţionale este obligat să întocmească următoarele proceduri de audit al sistemului:

    57.1 Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform datei şi timpului tentativei intrării/ieşirii, ID-ul utilizatorului şi rezultatului tentativei de intrare/ieşire (pozitivă sau negativă).

    57.2 Înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform datei şi timpului tentativei de pornire, denumirii/identificatorului programului aplicativ sau procesului, ID-ului utilizatorului, rezultatului tentativei de pornire (pozitivă sau negativă).

    57.3 Înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform datei şi timpului tentativei de obţinere a accesului (executare a operaţiunii), denumirii (identificatorul) aplicaţiei sau procesului, ID-ul utilizatorului, specificaţiilor resursei protejate (identificator, nume logic, nume fişier, număr etc), tipului operaţiunii solicitate (citire, înregistrare, ştergere etc), rezultatului tentativei de obţinere a accesului (executare a operaţiunii) - pozitivă sau negativă.

    57.4 Înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform datei şi timpul modificării competenţelor, ID-ului administratorului care a efectuat modificările, ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

58. 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.

59. 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.

60. 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.
61. Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz 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

62. Se asigură identificarea, înregistrarea şi înlăturarea deficienţelor mijloacelor de program destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor mijloacelor de program.

63. Se asigură protecţia contra infiltrării programelor dăunătoare mijloacelor de program destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

64. 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 care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale

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

66. 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

67. Copiile de rezervă ale informaţiei care conţine date cu caracter personal. Copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate odată la 24 ore, fiind păstrate cel puţin 1 an în locuri sigure, cu acces limitat.

68. 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. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

69. Incidentele de securitate a informaţiei sunt evenimente ce au dus sau ar fi putut duce la realizarea riscurilor de securitate a informaţiei, ca rezultat al eşecului în cadrul proceselor, sistemelor, oamenilor sau în rezultatul evenimentelor externe. Un incident se produce nu doar atunci când există impact asupra securităţii resurselor informaţionale (realizarea riscului) şi atunci când un asemenea impact este posibil (risc nerealizat).

70. Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal va trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

71. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntîrziată. Prelucrarea incidentelor include în mod obligator depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii iniţiale, precum şi crearea unei pârghii de evitare a ulterioarelor incidente asemănătoare. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

72. Anual, către 31 ianuarie, persoana responsabilă de Politica de securitate va prezenta Universităţii raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal.

73. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, semnatari a anexei nr. 2, pentru nerespectarea Politicii poartă răspundere civilă, contravențională și penală.