Politica notificată la Centrul Național
de Protecție a Datelor cu Caracter
Personal sub nr.

1362996528839

Anexa nr. 1
la ordinul CNTS
nr. 35-O din 04.09.16

POLITICA
de asigurare a securității datelor cu caracter personal în cadrul Centrului Național de Transfuzie a Sîngelui

PREAMBUL

Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale și mecanice de date cu caracter personal au drept scop stabilirea regulilor de implementare de către Centrul Național de Transfuzie a Sîngelui a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și mecanice de date cu caracter personal și/sau registrelor ținute manual, în conformitate cu prevederile Legii Nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, Nr. 170-175 art Nr : 492) și Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314) și Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European TreatySeries, nr. 108, ratificate de Republica Moldova prin Hotărîrea Parlamentului nr. 483-XIV din 2 iulie 1999.

I. DISPOZIȚII GENERALE

1. În sensul prezentei Politici, se definesc următoarele noțiuni:
autentificare– verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;
fișiere temporare – ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat pînă la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;
identificare– atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
integritate – certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;
mijloace de protecție criptografică a informației care conține date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;
politica de securitate a datelor cu caracter personal– document, elaborat de către Centrul Național de Transfuzie a Sîngelui, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținîndu-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și 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 și/sau tehnic al accesului;
persoana responsabilă de politica de securitate a datelor cu caracter personal– persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;
protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și 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) eng. informationaltechnology)– 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 caracter personal;
stocare – păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINŢE GENERALE

2. 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 Centrul Naţional de Transfuzie a Sîngelui (în continuare CNTS).
3. 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.
4. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale şi mecanice de date cu caracter personal ale CNTS se înfăptuiesc ţinîndu-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.
5.Sînt supuse protecţiei toate resursele informaţionale ale CNTS, care conţin date cu caracter personal, inclusiv:
1) suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
2) 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 tehnice de prelucrare a informaţiei.
6. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:
1) preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
2) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
3) respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
4) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
5) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.
7. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:
1) preîntîmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
3) preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea,

modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
4) 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.
8.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.
9. 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.
10. Ordinea de acces la informaţia care conţine date cu caracter personal, prelucrată în cadrul sistemelor informaţionale, se stabileşte prin Ordinul CNTS emis în acest sens şi conform Regulamentului sistemului informaţional utilizat.

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

11. Prin Ordinul CNTS nr. __ din „__" _____ 2016 este nominalizat responsabil de întocmirea, menţinerea, modificarea şi actualizarea politicii de securitate şeful Serviciului Juridic.
12. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal. În acest sens, la CNTS sunt create 2 sisteme informaţionale: SIA „Serviciul de Sînge" (CTS Manager) şi „Universal Acounting" şi unul mecanic al Serviciului Resurse Umane.
Se numeşte responsabil de administrarea SIA „Serviciul de Sînge" (CTS Manager) şeful Secţiei Tehnologii Informaţionale.
Se numeşte responsabil de administrarea SIA „Universal Acounting" deţinătorul funcţiei de şef Secţie Economie şi Evidenţă Contabilă.
13. Mecanismul de punere în aplicare a măsurilor de securitate este de prevăzut de prezenta Politică de Securitate;
14. Nomenclatorul datelor cu caracter personal prelucrate în cadrul CNTS este stabilit de Regulamentul de securitate al fiecărui sistem, care prelucrează date cu caracter personale.
15. Lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal este stabilită prin Ordinul intern al CNTS.
16. Configurarea sistemului informaţional de date cu caracter personal şi a reţelei are loc în conformitate cu cerinţele tehnice nr. 37603221.425790.078-00.PB.01.01;
17. Descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal prelucrate în registrul ţinut manual este prevăzută în Regulamentul politicii de securitate a datelor cu caracter personal al SRU;
18. Documentaţia tehnică cu privire la controalele de securitate este ţinută sub formă de registre de către persoana responsabilă, numită prin Ordinul CNTS pentru fiecare sistem informaţional în parte.
19. 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.
20. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoştinţa conducerii CNTS în mod de urgenţă, pentru a putea fi identificată procedura de soluţionare a incidentului.

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

Secţiunea 1
Autorizarea accesului fizic

21. Pentru categoria N-1

Accesul în sediile/oficiile/birourile ori spaţiile unde sînt 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.

22. Drept excepţie, în sălile de colectare a sîngelui/componentelor sanguine, sau control al posibililor donatori de sînge/componente sanguine este permis accesul persoanelor fizice doar la prezentarea fişa de donare eliberată la registratură. Aceste persoane vor fi în mod obligatoriu monitorizate de către personalul medical pe perioada aflării lor în birou, pentru a exclude careva acces la sistemele informaţionale.

23. Accesul în camera de servere este permisă doar personalului IT. Personalul străin are acces în această încăpere doar sub stricta supraveghere a unui specialist IT. Toate operaţiunile de acces la servere sau alte mijloace tehnice sau software se face de către personalul IT al CNTS.

Secţiunea 2
Administrarea şi monitorizarea accesului fizic

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

25.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.

26. Camera deservere este echipată cu uşă metalică şi gratii metalice la ferestre.

27. Toate fişele personale ale fiecărui angajat, inclusiv carnetele de muncă sunt păstrate în safeu metalic, ocrotit împotriva incendiilor.

Secţiunea 3
Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal

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

29. Pereţii exteriori ai încăperilor sînt rezistenţi, intrările echipate cu lacăte. Birourile amplasate la parter au ferestrele echipate cu gratii.

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

31.Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii.

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

33. 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.

Secţiunea 4
Controlul vizitatorilor

34. Donatorii de sînge şi alte persoane care accesează sediile CNTS sunt 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 cît mai urgent. Incidentul va fi adus la cunoştinţa STI imediat.

Secţiunea 5
Securitatea electroenergetică

35. Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

CNTS dispune de surse autonome de alimentare cu energie electrică de scurtă şi lungă 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.

Secţiunea 6

Securitatea cablurilor de reţea

36. Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Cablurile de tensiune sînt separate de cele comunicaţionale pentru a exclude bruiajul. Specialiştii IT al CNTS efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

Secţiunea 7

Asigurarea securităţii antiincendiare a sistemelor informaţionale de date cu caracter personal

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

Secţiunea 8

Controlul instalării şi scoaterii componentelor TI

38. Se exercită controlul şi 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.

Secţiunea 9

Măsurile generale de administrare a securităţii informaţionale

39.În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie. Computerele, terminalele de acces şi imprimantele sînt 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 soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Directorului CNTS.

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

Secţiunea 1

Identificarea şi autentificarea utilizatorului

40. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori. 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. Pentru confirmarea ID-ului utilizatorului sînt utilizate 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 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.

41. 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.).

Secţiunea 2

Identificarea şi autentificarea echipamentului

42. Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal.

Secţiunea 3

Administrarea identificatorilor utilizatorilor

43. Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticităţii fiecărui utilizator;

3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declaraţiei de confidenţialitate şi trecerii procedurii de instruire;

4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (2 săptămîni);

6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Secţiunea 4

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor

44. Se asigură conexiunea bilaterală a CNTS cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Secţiunea 5

Utilizarea parolelor în procesul asigurării securităţii informaţionale

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

1) păstrarea confidenţialităţii parolelor;

2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată cîndsînt prezente indiciile eventualei compromiteri a sistemului sau parolei;

4) 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;

5) modificarea parolelor peste intervale de maximum 40 zile;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Secţiunea 6

Administrarea parolelor utilizatorilor

46. Se folosesc 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

Secţiunea 1

Administrarea accesului

47. Se implementează 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.

Secţiunea 2

Administrarea conturilor de acces (account-urilor)

48. Este efectuată 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 (5 zile de inactivitate a contuului). Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Secţiunea 3

Acordarea accesului

49. Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu prezenta Politică de securitate persoanelor numite la pct. 11 şi 12.

Secţiunea 4

Revizuirea drepturilor de acces ale utilizatorilor

50. 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 5

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe

51. 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 CNTS 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.

Secţiunea 6

Informaţii de avertizare

52. 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.

Secţiunea 7

Blocarea sesiunii de lucru

53. 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.

Secţiunea 8

Controlul administrării accesului

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

Secţiunea 9

Marcarea documentelor

55. Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicîndu-se prescripţii pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deţinătorului de date cu caracter personal.

Secţiunea 10

Accesul de la distanţă

56. 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 CNTS şi este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Secţiunea 11

Limitarea folosirii tehnologiilor fără fir

57. 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 CNTS.

Secţiunea 12

Administrarea accesului echipamentului portativ şi mobil

58. Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil se documentează, este monitorizat şi controlat. Folosirea echipamentului portativ şi mobil este autorizată de Serviciul Tehnologii Informaţionale al CNTS.

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

Secţiunea 1

Divizarea programelor aplicative

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

Secţiunea 2

Izolarea funcţiilor de securitate

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

Secţiunea 3

Informaţia restantă

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

Secţiunea 4

Protecţia contra refuzului în serviciu

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

Secţiunea 5

Priorităţile resurselor

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

Secţiunea 6

Protecţia perimetrului sistemelor informaţionale încare sînt prelucrate date cu caracter personal

64. 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 a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

Secţiunea 7

Asigurarea integrităţii datelor cu caracter personal transmise

65. Se asigură integritatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de

protecţie criptografică.

Secţiunea 8
Asigurarea confidenţialităţii datelor cu caracter personal transmise

66. 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

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

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

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;

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

2) Este efectuată 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 următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau 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 negativă.

4) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

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

68. 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.

69. 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.

70. 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.

71. 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 1 an, 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
Înlăturarea deficienţelor de soft destinat prelucrăriidatelor cu caracter personal

72. 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
Asigurarea protecţiei contra programelor dăunătoare (virusilor)

73. Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile 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.

Secţiunea 3
Tehnologiile şi mijloacele de constatare a intruziunilor

74. 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.

Secţiunea 4
Asigurarea integrităţii soft-urilor şi informaţiei

75. 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.

Secţiunea 5
Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

76. 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
Copiile de rezervă ale informaţiei care conţine date cu caracter personal

77. 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 (safeu).

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

Secţiunea 1
Instructajul de reacţionare la incidentele de securitate a sistemelor informaţionale de date cu caracter personal

78. 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.

79. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntîrziată a conducerii CNTS.

80. Prelucrarea incidentelor include în mod obligator depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii iniţiale, precum şi crearea unei pîrghii de evitare a ulterioarelor incidente asemănătoare.

81. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

82. Anual, către 31 ianuarie, persoana responsabilă de Politica de securitate va prezenta Centrului Naţional pentru Protecţia Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal.