Anexa
La Ordinul nr. 01-19/238
Din 27.12.2017
***APROBAT*_____**

POLITICA DE SECURITATE

PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAŢIONALE GESTIONATE DE IMSP INSTITUTUL MAMEI ŞI COPILULUI

I. INTRODUCERE

Prezenta Politică este aprobată de către IMSP Institutul Mamei şi Copilului, care acţionează în baza Regulamentului IMSP Institutului Mamei şi Copilului şi are sediul înregistrat pe adresa: str. Burebista 93, mun. Chişinău, Republica Moldova.

Politica este aprobată, în vederea conformării IMSP Institutul Mamei şi Copilului cu prevederile Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului Republicii Moldova nr.1123 din data de 14 decembrie 2010 şi Legii Republicii Moldova nr.133 din 08.07.2011 privind protecţia datelor eu caracter personal.

La prelucrarea datelor cu caracter personal în cadrul IMSP Institutul Mamei şi Copilului sunt aplicate principiile prevăzute de actele internaţionale (Declaraţia Universală a Drepturilor Omului, Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Directiva 95/46/CE a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date) şi naţionale (Constituţia Republicii Moldova, Legea nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, Legea nr.982 din 11.05.2000 privind accesul la informaţie, Cerinţele faţă de asigurarea securităţii datelor cu acestora în cadrul sistemelor informaţionale de date cu caracter personal la prelucrarea caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012).

II. NOŢIUNI GENERALE

În prezenta Politică de Securitate, sunt definite/utilizate următoarele noţiuni:

date cu caracter personal - orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

categorii speciale de date cu caracter personal - datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancţiunile contravenţionale;

operator - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de Legislaiţia în vigoare;

persoană împuternicită de către operator - persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

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

control de securitate — acţiuni întreprinse de către Ministerul Sănătăţii, Muncii, Protecţiei Sociale în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

identificarea - atribuirea unui indentificator subecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

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

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal - mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

politica de securitate a datelor cu caracter personal - document, elaborat de către operatorul de date - IMSP Institutul Mamei şi Copilului, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinându-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sunt expuse acestea;

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 perspnal;

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 hârtie 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;

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 până 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;

prelucrarea datelor cu caracter personal - orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

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

sistem de evidenţă a datelor cu caracter personal - orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcţionale sau geografice;

consimţamintul subiectului datelor cu caracter personal — orice manifestare de voinţa liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

program de tip shareware - program care este furnizat gratuit pentru o perioadă limitată, dar care conţine restricţii de funcţionalitate, disponibilitate sau comoditate în utilizare;

program de tip freeware - program care sunt accesibile pentru a fi utilizate gratuit, pentru o perioadă nelimitată de timp.

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

Secţiunea 1
Obiectivele Politicii de securitate

1. Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de IMSP Institutul Mamei şi Copilului, atât în cadrul prelucrării manuale, cât și sistemelor şi proceselor de tehnologie informaţională.

2. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe TI în cadrul IMSP Institutul Mamei şi Copilului. Baza unei securităţi TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor TI împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv nemateriale (morale), sau care pot duce la încălcări ale legislaţiei.

3. Având în vedere că siguranţa TI nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico- juridic şi de altă natură.

4. IMSP Institutul Mamei şi Copilului va proteja datele cu caracter personal atât a participanţilor la proces/vizitatori, cât şi a angajaţilor săi.

5. Reglementările prezentei Politici reprezintă un standard minim pentru Ministerul Sănătăţii, Muncii și Protecției Sociale, inclusiv toţi angajaţii Ministerului Sănătăţii Muncii și Protecției Sociale.

6. Angajaţii IMSP Institutul Mamei şi Copilului urmează să respecte strict prevederile Politicii şi regulilor interne ale IMSP Institutul Mamei şi Copilului privind protecţia datelor cu caracter personal şi sistemelor TI.

Secţiunea 2
Scopul aplicării măsurilor de protecţie a datelor cu caracter personal

7. Măsurile de protecţie a datelor cu caracter personal sunt asigurate în scopul:

1) preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

2) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;

3) neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată;

4) eficientizarea resurselor informaţionale atât pe suport de hârtie cât şi cel în format electronic.

Secţiunea 3
Metodele de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale

8. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se ectuează prin următoarele metode:

1) preîntâmpinarea 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) preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

4) preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

5) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN;

6) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;

7) preîntâmpinarea 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;

8) stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atât pentru utilizatorii interni, cât şi pentru cei externi.

Secţiunea 4
Resursele informaţionale supuse principiilor de protecţie a datelor cu caracter personal

9. Protecţia datelor cu caracter personal în cadrul IMSP Institutul Mamei şi Copilului (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

10. Sunt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe:

1) suporturi 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.

Secţiunea 5
Dispoziţii privind ierarhia şi responsabilitatea persoanei responsabile de Politica de securitate

11. Operatorul de date cu caracter personal, reieşind din specificul activităţii, prin prezenta Politică de securitate, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.

12. Politica ae securitate a datelor cu caracter personal se va revizui cei puţin o dată în an ca rezultat al modificărilor sau reevaluării competenţelor entităţii, conducătorii vor desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

13. Politica de securitate, în mod obligatoriu este adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

14. Responsabil de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, este desemnată persoana, care conform fişei postului şi/sau ordinului intern, dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi are acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

15. Persoana responsabilă desemnată, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se subordonează nemijlocit conducătorului IMSP Institutul Mamei şi Copilului sau persoanei care îndeplineşte interimatul funcţiei.

16. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

17. Persoana responsabilă de politica de securitate a datelor cu caracter personal întreprinde următoarele acţiuni:

1) defineşte clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală;

2) asigură măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal;

3) elaborează procedurile de clasificare a informaţiei care conţine date cu caracter personal, astfel încât să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date;

4) instruieşte persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

Secţiunea 6
Procedurile organizatorice şi tehnice respectate în cadrul IMSP Institutul Mamei şi Copilului la prelucrarea datelor cu caracter personal

18. Măsurile generale de administrare a securităţii informaţionale:

1) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

2) Computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru.

3) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

4) Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

5) 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 conducerii.

6) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.

7) Este interzisă instalarea programelor de tip shareware sau freeware, aprobarea administratorului sistemului informatic.

Secţiunea 7
Securitatea mediului fizic, a sediilor/oficiilor şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

19. 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, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

20. Se asigură 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.

21. Perimetrul de securitate a IMSP Institutul Mamei şi Copilului reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal.

22. Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sunt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.

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

24. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

25. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

26. Accesul în perimetrul de securitate a clădirii IMSP Institutul Mamei şi Copilului unde se prelucrează/stochează daţe cu caracter personal cu utilaje foto/video neautorizate este interzis, ţinând cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 şi art. 30 ale Legii privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţe.

27. 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.

Secţiunea 8
Identificarea şi autentificarea utilizatorilor şi echipamentului. Administrarea identificatorilor utilizatorilor

28. Identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate este efectuată în numele acestor utilizatori.

29. Toţi utilizatorii (inclusliv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.

30. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

31. 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 sau se suspendă de administratorul TI.

32. Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator.
2) verificarea autenticităţii fiecărui utilizator.

33. Este asigurata posibilitatea identicarii şi autentifincării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioadă îndelungată

Secţiunea 9
Utilizarea parolelor în procesul asigurării securităţii informaţionale. Controlul administrării accesului.

34. În cazul alegerii şi folosirii parolelor sunt respectate regulile de asigurare a securităţii informaţionale, care includ:

1) păstrarea confidenţialităţii parolelor;
2) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestora;
3) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
4) 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 sunt compuse iritegral din grupuri de cifre sau litere;
5) modificarea parolelor jpeste intervale de 3 luni;
6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

35. Controlul sistematic al acţiunilor utilizatorilor este efectuat în scopul evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Secţiunea 10
Accesul de la distanţă.
Limitarea folosirii tehnologiilor fără fir

36. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sunt documentate, supuse monitorizării şi controlului.

37. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale IMSP Institutul Mamei şi Copilului şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

38. Accesul fără fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării şi controlului.

39. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

40. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale IMSP Institutul Mamei şi Copilului.

Secţiunea 11
Securitatea elcctroenergeticâ.
Controlul instalării şi scoaterii componentelor T.I.

41. Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

42. 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.

43. Sunt implementate sisteme automatizate de depistare şi semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

44. Este exercitat 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.

45. 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, evitându-se folosirea funcţiilor standarde de nimicire.

Secţiunea 12
Dezvăluirea datelor cu caracter personal

46. Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN.

47. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi.

48. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmînarea personală, etc.).

49. Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor (expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.).

50. Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între IMSP Institutul Mamei şi Copilului şi alte entităţi amplasate geografic în stânga Nistrului, care nu se află în administrarea jurisdicţională a Republicii Moldova.

51. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie şi/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituţional/acord bilateral, luându-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.

52. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în special în cazurile când tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

53. Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidenţei IMSP Institutul Mamei şi Copilului, este limitat la strictul necesar pentru realizarea scopurilor declarate.

54. Acces la sistemele informaţionale gestionate în cadrul IMSP Institutul Mamei şi Copilului, din partea Procuraturii Generale (procuraturile teritorial e/specializate), Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie, va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală.

Se explică că, în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adeverite circumstanţe care au importanţă pentru cauză (inclusiv; informaţia stocată în auditul sistemelor informaţionale şi de evidenţă), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei, cu respectarea prevederilor art. 214 Cod de procedură penală.

55. În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fişa personală a clientului, aceştia vor fi informaţi în scris despre obligaţiile ce le revin, în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind proiecţia datelor cu caracter personal, inclusiv despre răspunderea prevazută de art. 74 Cod contravenţional.

Secţiunea 13
Drepturile subiecţilor de date cu caracter personal

56. În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecţia datelor cu caracter personal, este necesar de a-i furniza următoarele informaţii, exceptând cazul în care subiectul deţine deja informaţiile respective:

1) privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidenţă al operatorilor de date cu| caracter personal);

2) privind scopul concret al prelucrării datelor cu caracter personal colectate;

3) privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

4) dreptul la informare şi pe acces la datele colectate, de intervenţie asupra datelor (de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia;

5) dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine.

57. Persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţii subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

58. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigură mentenanţa sistemului şi sau prestează servicii extemalizate ale operatorului) tuturor persoanelor supuse prelucrării.

59. În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat, etc.), modificarea se va efectua în toate sistemele informaţionale şi de evidenţă gestionate.

Secţiunea 14
Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

60. Accesul în spaţiile/perimetrul unde sunt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale/regulamentelor departamentale aprobate.

61. Este interzisă stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de: evidenţă, în computere care sunt conectate la internet şi nu sunt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului.

62. Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă.

63. Accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredinţate doar persoanei responsabile pentru implementarea Polticii de securitate desemnate din cadrul IMSP Institutul Mamei şi Copilului.

64. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie 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, este asigurat prin plasarea acestora în şafeuri sau dulapuri metalice care se încuie.

65. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

Secţiunea 15
Auditul sistemelor informaţionale gestionate

66. Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem se efectuează conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

67. Înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal se efectuează conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executate a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau procesului, o ID-ul utilizatorului;
c) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
d) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
e) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

68. Înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, este efectuată 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.

69. Înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etic.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces se efectuează 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.

Secţiunea 16
Asigurarea protecţiei contra programelor dăunătoare (viruşilor). Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

70. Protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existența a programelor de antivirus.

71. Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal automat - la pornirea șistemului şi lunar - la solicitarea utilizatorului autorizat în acest scop.

Secţiunea 17
Gestionarea incidentelor de securitate

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

73. Personalul IMSP Institutul Mamei şi Copilului informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

74. Prelucrarea incidentelor include: depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

75. Până la data de 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Autoritatea naţională pentru protecţia datelor cu caracter personal despre incidentele de securitate constatate.

Secţiunea 18
Marcarea documentelor. Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal şi a informaţiilor cu accesibilitate limitată

76. Toată informaţia care se intenţionează a fi dezvăluită, şi care conţine date cu caracler personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidenţă al operatorilor de date cu caracter personal.

Model: „Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. 000000X-00X, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter persopal”,

77. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe, după caz, semnatari ai anexei nr. 1, pentru nerespectarea dispoziţiilor Politicii de securitate - poartă răspundere civilă, contravenţională şi penală conform prevederilor legislaţiei în vigoare.

Secțiunea 19
Dispoziții finale

78. Prezenta Politică este revizuită și ulterior aprobată de către conducerea IMSP Institutul Mamei și Copilului periodic, cel puțin o dată în an, precum și la necesitate.

79 Prezenta Politică se completează cu prevederile legislației în vigoare.

80 Prezenta Politică este adus la cunoștința angajaților contra semnăturii.

81 Modificarea și completarea Politici se face în modul stabilit pentru aprobarea ei.