

**APROB**  
**Vicedirector I.M. INFOCOM**

**Adrian Malic**

**Data** 10.03.2011

**Semnătura** \_\_\_\_\_



## **Politica instituțională de securitate a datelor cu caracter personal în cadrul IM Infocom.**

### **I. DISPOZIȚII GENERALE**

Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal în IM INFOCOM au drept scop stabilirea regulilor minime de implementare de către IM INFOCOM a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale de date cu caracter personal și registrelor ținute manual, în conformitate cu prevederile Legii nr.17-XVI din 15 februarie 2007 cu privire la protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2007, nr.107-111, art.468) și ale Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314).

### **II. CERINȚE GENERALE**

1. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului informațional de date cu caracter personal în cadrul IM INFOCOM și vor fi efectuate neîntreput .
2. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal în cadrul IM INFOCOM este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
3. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale de date cu caracter personal în cadrul IM INFOCOM se îndeplinesc ținându-se cont de necesitatea asigurării confidențialității acestor măsuri.
4. Îndeplinirea oricăror măsuri și lucrări cu folosirea resurselor informaționale este interzisă în cazurile în care nu sînt adoptate și implementate măsuri corespunzătoare de protecție a datelor cu caracter personal.
5. Sînt supuse protecției toate resursele informaționale, care conțin date cu caracter personal, inclusiv:
  - 1) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
  - 2) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.
6. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în scopul:
  - 1) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
  - 2) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

3) respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;

4) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;

5) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

7. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

1) preîntâmpinarea conexiunilor neautorizate la rețelele comunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;

3) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

4) preîntâmpinarea acțiunilor intenționate și neintenționate a utilizatorilor interni sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

8. Preîntâmpinarea accesului neautorizat la informațiile care conțin date cu caracter personal și circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice și de program, cifrării acestor informații, inclusiv prin măsurile organizaționale și de regim.

9. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță.

10. Ordinea de acces la informația care conține date cu caracter personal, prelucrată în cadrul sistemelor informaționale, se stabilește de către administrația IM INFOCOM, în conformitate cu prevederile legislației.

### **III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL**

11. IM INFOCOM, reieșind din specificul activității, elaborează și organizează implementarea prevederilor documentului care stabilește politica de securitate a datelor cu caracter personal, inclusiv procedurile și măsurile legate de realizarea acestei politici, cu aplicarea soluțiilor practice cu un nivel de detalizare și complexitate proporțional, în partea ce ține de identificarea și autentificarea utilizatorilor; de reacționare la incidentele de securitate; de protecție a TI și comunicațiilor; de asigurare a integrității informației care conține date cu caracter personal și TI; de administrare a accesului; de audit și asigurare a evidenței, luând în considerare:

1) categoria datelor cu caracter personal prelucrate și a operațiunilor de prelucrare efectuate asupra lor;

2) dimensiunea datelor, în funcție de numărul angajaților, numărul organizațiilor contractate, numărul de apartamente, inclusiv numărul persoanelor care pot accesa datele cu caracter personal;

3) formele de ținere a registrelor în care sînt prelucrate date cu caracter personal (manuală, electronică sau mixtă);

4) complexitatea sistemelor informaționale de date cu caracter personal și programelor de aplicații implicate în procesul de prelucrare a datelor;

5) riscurile la care este expus IM INFOCOM sau persoanele ale căror date cu caracter personal sînt prelucrate, starea de dezvoltare tehnologică în acest domeniu și costul măsurilor de implementare.

12. Politica de securitate a datelor cu caracter personal se revizuieste o dată în an ca rezultat al modificărilor sau reevaluării componentelor acesteia și aprobată la cel mai înalt nivel al ierarhiei persoanelor responsabile ale deținătorului de date cu caracter personal.

Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoștință utilizatorilor și altor angajați ai deținătorului de date cu caracter personal, în limitele competențelor funcționale și nivelului de acces acordat.

13. Este numita o persoană responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituției, care nu va avea alte responsabilități incompatibile cu sarcinile funcției de implementare a politicii.

14. Persoana responsabilă de politica de securitate a datelor cu caracter personal va dispune de resurse suficiente (timp, resurse umane, echipament și buget) și are acces liber la informația necesară pentru îndeplinirea funcțiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

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

#### 16. IM INFOCOM:

1) definește clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală;

2) asigură măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal;

3) elaborează procedurile de clasificare a informației care conține date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator și toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;

4) instruieste persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

17. Documentația referitoare la politica de securitate a datelor cu caracter personal este centralizată, completă, actualizată cu regularitate și conține cel puțin următoarele elemente:

1) identitatea persoanei responsabile de politica de securitate;

2) măsurile de securitate;

3) mecanismul de punere în aplicare a măsurilor de securitate;

4) nomenclatorul datelor cu caracter personal prelucrate, a localizării acestora și a operațiunilor efectuate asupra lor;

5) lista nominală a utilizatorilor, autorizați să acceseze datele cu caracter personal;

6) configurarea sistemului informațional de date cu caracter personal și a rețelei;

7) descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal prelucrate în registrul ținut manual;

8) documentația tehnică cu privire la controalele de securitate;

9) orarul controalelor de securitate;

10) măsurile de detectare a cazurilor de acces și de prelucrare neautorizată a datelor cu caracter personal;

11) rapoarte despre incidentele de securitate.

## IV. SECURITATEA MEDIULUI FIZIC ȘI A TEHNOLOGIILOR INFORMAȚIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Autorizarea accesului fizic

Accesul în sediul IM INFOCOM și spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, conform listei și însemnelor corespunzătoare. Administrația elaborează și aprobă listele de acces, care se revizuiesc după necesitate.

### **Administrarea și monitorizarea accesului fizic**

Se efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

Înainte de acordarea accesului fizic la sistemele informaționale de date cu caracter personal se verifică competențele de acces.

### **Securitatea sediului, birourilor și mijloacelor de prelucrare a datelor cu caracter personal**

Perimetrul de securitate se determină concret și clar. Perimetrul clădirii și încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt integri din punct de vedere fizic.

Pereții exteriori ai încăperilor sunt rezistenți, intrările echipate cu lacăte, mijloace de control al accesului, semnalizare.

Computerele, serverele, sunt amplasate în locuri cu acces limitat pentru persoane străine.

Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc angajații.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal răspund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

### **Controlul vizitatorilor**

Accesul fizic al vizitatorilor în încăperile unde sînt amplasate sistemele informaționale de date cu caracter personal este interzis.

### **Securitatea electroenergetică**

Este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate.

În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

Sunt prevăzute 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.

### **Securitatea cablurilor de rețea**

Cablurile de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancționate sau deteriorărilor.

### **Asigurarea securității antiincendiare a sistemelor informaționale de date cu caracter personal**

Sunt prevăzute mijloace de asigurare a securității antiincendiare a sediilor șibirourilor unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

### **Controlul instalării și scoaterii componentelor TI**

Se exercită controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire.

### **Măsurile generale de administrare a securității informaționale**

În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.

Computerele, terminalele de acces și imprimantele sînt deconectate la terminarea sesiunilor de lucru.

Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.

Trebuie administrat accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.

Mijloacele de prelucrare a datelor cu caracter personal, informația care conține 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 conducerii deținătorului de date cu caracter personal.

## **V. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL**

### **Identificarea și autentificarea utilizatorului**

Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.

Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmintele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces

cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.

În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și 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 permise în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de către deținătorul de date cu caracter personal.

### **Identificarea și autentificarea echipamentului**

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal.

### **Administrarea identificatorilor utilizatorilor**

Administrarea identificatorilor utilizatorilor include:

- 1) identificarea univocă a fiecărui utilizator;
- 2) verificarea autenticității fiecărui utilizator;
- 3) obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;
- 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 (inacțiune în perioada de maximum 2 luni);
- 6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

### **Administrarea mijloacelor de autentificare**

Deținătorii de date cu caracter personal determină procedurile administrative, care reglementează procesul distribuirii și ridicării mijloacelor de autentificare a utilizatorilor, inclusiv acțiunile în cazul pierderii/compromiterii sau defecțiunii acestora.

După instalarea sistemului, se schimbă informațiile de autentificare a utilizatorilor utilizate standard.

### **Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor**

Se asigură conexiunea bilaterală a deținătorului de date cu caracter personal cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

### **Utilizarea parolelor în procesul asigurării securității informaționale**

Se respectă regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- 1) păstrarea confidențialității parolelor;
- 2) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- 3) modificarea parolelor de fiecare dată când sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- 4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu

sînt compuse integral din grupuri de cifre sau litere;

5) modificarea parolelor peste intervale de maximum 3 luni;

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

### **Administrarea parolelor utilizatorilor**

Se folosesc identificatoare individuale pentru fiecare utilizator și parole individuale ale acestora pentru asigurarea posibilității de stabilire a responsabilității.

Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora.

Se asigură blocarea accesului după trei tentative greșite de autentificare.

Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioadă de un an) și prevenirea folosirii repetate a acestora.

La momentul introducerii, parolele nu se reflectă în clar pe monitor.

Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral (funcția hash).

## **VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR**

### **Administrarea accesului**

Se implementează mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

### **Administrarea conturilor de acces (account-urilor)**

Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora.

Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces.

Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte).

Sînt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor neactivi, care prelucrează date cu caracter personal.

Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

### **Acordarea accesului**

Este autorizat accesul la sistemele informaționale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deținătorul de date cu caracter personal.

Accesul la funcțiile de securitate ale sistemelor informaționale de date cu caracter personal și la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deținătorului de date cu caracter personal.

### **Revizuirea drepturilor de acces ale utilizatorilor**

Drepturile de acces ale utilizatorilor la sistemele informaționale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare șase luni) și după oricare schimbare de statut al

utilizatorului.

### **Administrarea fluxurilor informaționale**

Se autorizează de către deținătorii de date cu caracter personal realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul și în afara sistemelor informaționale de date cu caracter personal.

### **Repartizarea obligațiilor și investirea cu minimumul de drepturi și competențe**

Repartizarea obligațiilor subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul investiției cu drepturi/competențe corespunzătoare de acces, printr-un act administrativ al conducerii deținătorului de date cu caracter personal.

Utilizatorii sistemelor informaționale de date cu caracter personal se investesc doar cu acele drepturi/competențe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

### **Informații de avertizare**

Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.

### **Blocarea sesiunii de lucru**

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

### **Controlul administrării accesului**

Se efectuează controlul acțiunilor utilizatorului în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

### **Marcarea documentelor**

Informația ieșită din sistem, care conține date cu caracter personal, se marchează, indicîndu-se prescripții pentru prelucrarea ulterioară și răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deținătorului de date cu caracter personal.

### **Accesul de la distanță**

Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sînt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum și sînt documentate, supuse monitorizării și controlului.



Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal se autorizează de persoanele responsabile ale deținătorilor de date cu caracter personal și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

### **Limitarea folosirii tehnologiilor fără fir**

Accesul fără fir la sistemele informaționale de date cu caracter personal nu este folosit.

### **Administrarea accesului echipamentului portativ și mobil**

Accesul la sistemele informaționale de date cu caracter personal cu folosirea echipamentului portativ și mobil nu se folosește

## **VII. PROTECȚIA SISTEMELOR INFORMAȚIONALE ȘI COMUNICAȚIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL**

### **Divizarea programelor aplicative**

Este asigurată separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale de date cu caracter personal.

### **Izolarea funcțiilor de securitate**

Este asigurată izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale de date cu caracter personal.

### **Informația restantă**

Sunt preîntâmpinate tentativele dezvăluirii neautorizate sau neintenționate a informației restante care conține date cu caracter personal, prin intermediul resurselor informaționale general accesibile.

### **Protecția contra refuzului în serviciu**

Se asigură protecția sistemelor informaționale de date cu caracter personal sau limitate posibilitățile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) - „refuz în serviciu”.

### **Prioritățile resurselor**

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

## **Protecția perimetrului sistemelor informaționale în care sînt prelucrate date cu caracter personal**

Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale.

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

### **Asigurarea integrității datelor cu caracter personal transmise**

Se asigură integritatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de protecție criptografică și semnătura digitală.

### **Asigurarea confidențialității datelor cu caracter personal transmise**

Se asigură confidențialitatea datelor cu caracter personal transmise, utilizîndu-se mijloace de protecție criptografică a informației.

## **VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

### **Generarea înregistrărilor de audit în sistemele informaționale de date cu caracter personal**

Deținătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

#### **Lista evenimentelor înregistrate de sistemul de audit a securității în sistemele informaționale de date cu caracter personal**

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

- a) data și timpul tentativei intrării/ieșirii;
- b) ID-ul utilizatorului;
- c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.

2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

- a) data și timpul tentativei de pornire;
- b) denumirea/identificatorul programului aplicativ sau procesului;
- c) ID-ul utilizatorului;
- d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
  - b) denumirea (identificatorul) aplicației sau procesului;
  - c) ID-ul utilizatorului;
  - d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
  - e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
  - f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.
- 4) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- a) data și timpul modificării competențelor;
  - b) ID-ul administratorului care a efectuat modificările;
  - c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- 5) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
- a) data și timpul eliberării;
  - b) denumirea informației și căile de acces la aceasta;
  - c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
  - d) ID-ul utilizatorului, care a solicitat informația;
  - e) volumul documentului eliberat (numărul paginilor, a fișierelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

#### **Prelucrarea rezultatelor auditului securității în sistemele informaționale de date cu caracter personal**

În caz de deranjament al auditului securității în sistemele informaționale 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 și întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

#### **Monitorizarea, analiza și generarea rapoartelor de audit a securității în sistemele informaționale de date cu caracter personal**

Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul și întreprinderea acțiunilor prestabilite în politica de securitate pentru astfel de cazuri.

#### **Protejarea datelor de audit a securității în sistemele informaționale de date cu caracter personal**

Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.

#### **Păstrarea datelor de audit a securității în sistemele informaționale de date cu caracter personal**

Durata stocării rezultatelor auditului securității în sistemele informaționale 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 investigații sau procese judiciare.

În cazul în care investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

## **IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI A TEHNOLOGIILOR INFORMAȚIONALE**

### **Înlăturarea deficiențelor de soft destinat prelucrării datelor cu caracter personal**

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

### **Asigurarea protecției contra programelor dăunătoare (virusilor)**

Se asigură protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și semnăturilor de virus.

### **Asigurarea integrității soft-urilor și informației**

Se asigură protecția și posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal și informației care conține date cu caracter personal.

Soft-urile destinate prelucrării datelor cu caracter personal și informația care conține date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sînt securizate prin metoda folosirii semnăturii digitale.

### **Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal**

Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

## **X. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI IT**

### **Copiile de rezervă ale informației care conține date cu caracter personal**

Copii de siguranță se efectuează zilnic..

Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației care conține date cu caracter personal.

Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate,

în scopul asigurării eficacității acestora.

Copiile de siguranță se păstrează în cutii metalice și în afara zonei de amplasare a informației care conține date cu caracter personal de soft-urile de bază , în încăperi din altă clădire.

## **XI. CONTROALELE DE SECURITATE A SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

Se verifică cu regularitate, cel puțin o dată pe an, îndeplinirea măsurilor tehnice și organizaționale luate pentru detectarea unor disfuncționalități în ceea ce privește folosirea în procesul prelucrării datelor cu caracter personal și efectuarea îmbunătățirilor, în caz de necesitate.

Controalele de securitate sînt actualizate de fiecare dată cînd are loc reorganizarea sau schimbul infrastructurii.

## **XII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

### **Instructajul de reacționare la incidentele de securitate a sistemelor informaționale de date cu caracter personal**

Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

### **Prelucrarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal**

Este asigurat mecanismul de informare neîntîrziată a conducerii despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.

Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

### **Monitorizarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal**

Incidentele de securitate a sistemelor informaționale de date cu caracter personal se urmăresc și se documentează în regim permanent.

### **Prezentarea rapoartelor despre incidentele de securitate a sistemelor informaționale de date cu caracter personal**

Annual, către 31 ianuarie, este prezentat Centrului raportul generalizat despre incidentele de securitate a sistemelor informaționale de date cu caracter personal.

