APROB
Vicedirector I.M. INFOCOM
Adrian Malic
Data _____
Semnătura _____

Politica instituţională de securitate a datelor cu caracter personal în cadrul I.M. Infocom.

(modificat 2023)

I. DISPOZIŢII GENERALE

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal în IM INFOCOM au drept scop stabilirea regulilor minime de implementare de către IM INFOCOM a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal, prelucrate în cadrul sistemelor informaţionale de date cu caracter personal şi registrelor ţinute manual, în conformitate cu prevederile Legii Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, Legii Nr. 229 din 23.09.2010 privind controlul financiar public intern, HG Nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

II. CERINŢE GENERALE

1. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemului informaţional de date cu caracter personal în cadrul IM INFOCOM şi vor fi efectuate neîntrerupt .

2. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal în cadrul IM INFOCOM este asigurată printr-un complex de măsuri tehnice şi organizatorice de preântâmpinare a prelucrării ilicite a datelor cu caracter personal.

3. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale de date cu caracter personal în cadrul IM INFOCOM se înfăptuiesc ţinîndu-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.

4. Înfăptuirea oricăror măsuri şi lucrări cu folosirea resurselor informaţionale este interzisă în cazurile în care nu sînt adoptate şi implementate măsuri corespunzătoare de protecţie a datelor cu caracter personal.

5. Sînt supuse protecţiei toate resursele informaţionale, 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) preântâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
2) preântâmpinării 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) preântâmpinarea conexiunilor neautorizate la reţelele comunicaţionale 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) preântâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
4) preântâmpinarea acţiunilor intenţionate şi neintenţionate a utilizatorilor interni 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. Preântâmpinarea accesului neautorizat la informaţiile care conţin date cu caracter personal şi circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice şi de program, cifrării acestor informaţii, inclusiv prin măsurile organizaţionale şi de regim.

9. Preântâmpinarea 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 de către administratia IM INFOCOM, în conformitate cu prevederile legislaţiei.

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

11. IM INFOCOM, reieşind din specificul activităţii, elaborează şi organizează implementarea prevederilor documentului care stabileşte politica de securitate a datelor cu caracter personal, inclusiv procedurile şi măsurile legate de realizarea acestei politici, cu aplicarea soluţiilor practice cu un nivel de detalizare şi complexitate proporţional, în partea ce ţine de identificarea şi autentificarea utilizatorilor; de reacţionare la incidentele de securitate; de protecţie a TI şi comunicaţiilor; de asigurare a integrităţii informaţiei care conţine date cu caracter personal şi TI; de administrare a accesului; de audit şi asigurare a evidenţei, luând în considerare:
1) categoria datelor cu caracter personal prelucrate şi a operaţiunilor de prelucrare efectuate asupra lor;
2) dimensiunea datelor, în funcţie de numărul angajaţilor, numărul organizaţiilor contractate, numărul de apartamente, inclusiv numărul persoanelor care pot accesa datele cu caracter personal;
3) formele de ţinere a registrelor în care sânt prelucrate date cu caracter personal (manuală, electronică sau mixtă);
4) complexitatea sistemelor informaţionale de date cu caracter personal şi programelor de aplicaţii implicate în procesul de prelucrare a datelor;
5) riscurile la care este expus IM INFOCOM sau persoanele ale căror date cu caracter personal sânt prelucrate, starea de dezvoltare tehnologică în acest domeniu şi costul măsurilor de implementare.

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

Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoştinţă utilizatorilor şi altor angajaţi ai deţinătorului de date cu caracter personal, în limitele competenţelor funcţionale şi nivelului de acces acordat.

13. Este numita o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei 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 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 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.

16. IM INFOCOM:

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 încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sânt 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.

17. Documentaţia referitoare la politica de securitate a datelor cu caracter personal este centralizată, completă, actualizată cu regularitate şi conţine cel puţin 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 şi a operaţiunilor efectuate asupra lor;
5) lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal;
6) configurarea sistemului informaţional de date cu caracter personal şi a reţelei;
7) descrierea detaliată a criteriilor, în conformitate cu care sânt accesibile datele cu caracter personal prelucrate în registrul ţinut manual;
8) documentaţia tehnică cu privire la controalele de securitate;
9) orarul controalelor de securitate;
10) măsurile de detectare a cazurilor de acces şi de prelucrare neautorizată a datelor cu caracter personal;
11) rapoarte despre incidentele de securitate.

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

Autorizarea accesului fizic

Accesul în sediul IM INFOCOM şi spaţiile unde sânt 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.

Administraţia elaborează şi aprobă listele de acces, care se revizuiesc după necesitate.

Administrarea şi monitorizarea accesului fizic

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

Înainte de acordarea accesului fizic la sistemele informaţionale de date cu caracter personal se verifică competenţele de acces.

Securitatea sediului, birourilor şi mijloacelor de prelucrare a datelor cu caracter personal

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

Pereţii exteriori ai încăperilor sunt rezistenţi, intrările echipate cu lacăte, mijloace de control al accesului, semnalizare

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

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

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

Controlul vizitatorilor

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

Securitatea electroenergetică

Este asigurată 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.

Sunt prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sânt 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 reţea

Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancţionate sau deteriorărilor.

Asigurarea securităţii antiincendiare a sistemelor informaţionale de date cu caracter personal

Sunt prevăzute mijloace de asigurare a securităţii antiincendiare a sediilor şibirourilor unde sânt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Controlul instalării şi scoaterii componentelor TI

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, evitându-se folosirea funcţiilor standarde de nimicire.

Măsurile generale de administrare a securităţii informaţionale

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 sânt 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.

Trebuie administrat accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sânt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii deţinătorului de date cu caracter personal.

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

Identificarea şi autentificarea utilizatorului

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) vor avea un identificator personal (ID-ul

utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sânt 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.

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 către deţinătorul de date cu caracter personal.

Identificarea şi autentificarea echipamentului

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

Administrarea identificatorilor utilizatorilor

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;
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 (inacţiune în perioada de maximum 2 luni);
6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Administrarea mijloacelor de autentificare

Deţinătorii de date cu caracter personal determină procedurile administrative, care reglementează procesul distribuirii şi ridicării mijloacelor de autentificare a utilizatorilor, inclusiv acţiunile în cazul pierderii/compromiterii sau defecţiunii acestora.

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

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor

Se asigură conexiunea bilaterală a deţinătorului 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 securităţii informaţionale

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 hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată când sânt prezente indiciile eventualei compromiteri a sistemului sau parolei;
4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sânt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sânt 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 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, utilizându-se algoritmul criptografic unilateral (funcţia hash).

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului

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.

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 şi ştergerea acestora.

Acţiunea 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).

Sânt 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 şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Acordarea accesului

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

Accesul la funcţiile de securitate ale sistemelor informaţionale de date cu caracter personal şi la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deţinătorului de date cu caracter personal.

Revizuirea drepturilor de acces ale utilizatorilor

Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sânt 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.

Administrarea fluxurilor informaţionale

Se autorizează de către deţinătorii de date cu caracter personal realizarea fluxurilor informaţionale în procesul transmiterii acestora în interiorul şi în afara sistemelor informaţionale de date cu caracter personal.

Repartizarea obligaţiilor şi investirea cu minimul de drepturi şi competenţe

Repartizarea obligaţiilor subiecţilor, care asigură funcţionarea sistemelor informaţionale de date cu caracter personal, este efectuată prin intermediul investirii cu drepturi/competenţe corespunzătoare de acces printr-un act administrativ al conducerii deţinătorului de date cu caracter personal.

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

Informaţii de avertizare

Înainte de acordarea accesului în sistem, utilizatorii sânt 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.

Blocarea sesiunii de lucru

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

Controlul administrării accesului

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

Marcarea documentelor

Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicându-se prescripţii pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv prin indicarea numărului de identificare unic al deţinătorului de date cu caracter personal.

Accesul de la distanţă

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

Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Limitarea folosirii tehnologiilor fără fir

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

Administrarea accesului echipamentului portativ şi mobil

Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil nu se foloseşte.

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

Divizarea programelor aplicative

Este asigurată separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

Izolarea funcţiilor de securitate

Este asigurată izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.

Informaţia restantă

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

Protecţia contra refuzului în serviciu

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".

Priorităţile resurselor

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

Protecţia perimetrului sistemelor informaţionale în care sânt prelucrate date cu caracter personal

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.

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

Asigurarea integrităţii datelor cu caracter personal transmise

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

Asigurarea confidenţialităţii datelor cu caracter personal transmise

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

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

Generarea înregistrărilor de audit în sistemele informaţionale de date cu caracter personal

Deţinătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

Lista evenimentelor înregistrate de sistemul de audit a securităţii în sistemele informaţionale de date cu caracter personal

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.

5. Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului, care a solicitat informaţia;
e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

Prelucrarea rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal

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.

Monitorizarea, analiza şi generarea rapoartelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

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 şi întreprinderea acţiunilor prestabilite în politica de securitate pentru astfel de cazuri.

Protejarea datelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

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.

Păstrarea datelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

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

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

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

Înlăturarea deficienţelor de soft destinat prelucrării datelor cu caracter personal

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.

Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reânnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

Asigurarea integrităţii soft-urilor şi informaţiei

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.

Soft-urile destinate prelucrării datelor cu caracter personal şi informaţia care conţine date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sânt securizate prin metoda folosirii semnăturii digitale.

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

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

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

Copiile de rezervă ale informaţiei care conţine date cu caracter personal

Copii de siguranţă se efectuiază zilnic.

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.

Copiile de siguranţă se păstrează în cutii metalice şi în afara zonei de amplasare a informaţiei care conţine date cu caracter personal de soft-urile de bază , în încăperi din altă clădire.

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

Se verifică cu regularitate, cel puţin o dată pe an, îndeplinirea măsurilor tehnice şi organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal şi efectuarea îmbunătăţirilor, în caz de necesitate.

Controalele de securitate sânt actualizate de fiecare dată când are loc reorganizarea sau schimbul infrastructurii.

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

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

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.

Prelucrarea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal

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

Prelucrarea incidentelor include depistarea, analiza, preântâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

Monitorizarea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal

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

Prezentarea rapoartelor despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal

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

Executor G. Eremei