

APROBAT:
Şef interimar al Direcției generale asistență
socială și sănătate a Consiliului municipal
Chișinău
Irina Banova
"19" aprilie 2018



L.Ş.

Redactată în baza ordinului
Şefului interimar al Direcției
nr.84-b din data 19.04.2018

**REGULAMENTUL
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ DIN CADRUL
DIRECȚIEI GENERALE ASISTENȚĂ SOCIALĂ ȘI SĂNĂTATE A CONSILIULUI
MUNICIPAL CHIȘINĂU**

I. DISPOZIȚII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (în continuare Regulament) este elaborat în vederea implementării în cadrul Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău a prevederilor Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău în cadrul sistemului de evidență contabilă.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă constă în asigurarea înregistrării informațiilor contabile referitoare la calculul drepturilor salariale ale angajaților, inclusiv a premiilor, stimulărilor, sporurilor, indemnizațiilor, ajutoarelor materiale, compensațiilor și altor drepturi și obligații cu conținut pecuniar, precum și a prezentării rapoartelor financiare, trimestriale și anuale către instituțiile statului, conform legislației în vigoare.

2.2. În cadrul sistemului de evidență contabilă sînt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- cetățenia și numărul personal de identificare de stat (IDNP);
- data și locul nașterii, domiciliul;
- sexul și datele din actele de stare civilă;
- codul personal de asigurări sociale (CPAS);
- codul personal de asigurări medicale (CPAM)

- datele privind locul de muncă și funcția ocupată;
- formarea profesională și sancțiuni disciplinare;
- imaginea și semnătura;
- datele din permisul de conducere;
- mărimea salariului brut și alte premii, sporuri, stimulări, suplimente;
- datele privind situația familială (la cererea solicitantului);
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- datele pentru transferul pe contul bancar a plăților salariale și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;
- mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

2.3. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

- a) Prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău intră în relații contractuale;
- b) Calcularea drepturilor salariale lunare, în conformitate cu legislația în vigoare a Republicii Moldova (conform contractelor individuale de muncă, contractelor civile, tabelelor de pontaj, ordinelor/dispozițiilor conducerii, raportului de activitate lunară);
- c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă;
- d) Prelucrarea copiilor ordinelor/dispozițiilor conducerii referitoare la personal;
- e) Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;
- f) Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului;
- g) Calcularea și virarea compensațiilor nominale pentru transport, în cazuri stabilite de legislației;
- h) Calcularea și virarea compensațiilor nominale pentru servicii funerare, în cazuri stabilite de legislației;
- i) Calcularea și virarea, conform listelor nominale, pentru servicii de cantină socială, în cazuri stabilite de legislației;
- j) Furnizarea informației necesare pentru elaborarea rapoartelor lunare privind contribuțiile de asigurare socială de stat obligatorii (forma 4BASS) și rapoartelor trimestriale privind primele de asigurare obligatorie de asistență medicală (Formularul MED08);
- k) Întocmirea, lunară, a declarației persoanei asigurate REV 5 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, în format electronic prin SIA E-REPORTING cu aplicarea semnăturii digitale;

- l) Asistarea procesului (prin furnizarea informației necesare) pentru completarea periodică (lunară) a raportului și dării de seamă privind venitul achitat și impozitul pe venit reținut din acesta;
- m) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat (privind impozitul pe venit IRV 14, TFD 13, IALS 14, MED 08), precum și perfectarea și eliberarea informației privind veniturile calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău;
- n) Prelucrarea cererilor și a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reținut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal, fiind completat și stocat Registrului de evidență a cererilor pentru scutiri la impozitul pe venit.
- o) Eliberarea certificatelor de salariu, la cererea angajaților;
- p) Completarea și stocarea fișelor personale de evidență a veniturilor sub formă de salariu și alte plăți efectuate de către patron în folosul angajatului pe fiecare an, precum și a impozitului pe venit reținut din aceste plăți (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007);
- q) Emiterea, transmiterea și primirea documentelor financiar-contabile (facturi, anexe la facturi, documente justificative, acte de prestare servicii);
- r) Prezentarea documentelor financiare ce conțin date cu caracter personal către auditului intern sau extern. În cazul datelor cu caracter personal ale angajaților sau ale altor persoane cu care Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău se află în relație juridică, îi va înștiința pe acești atunci când datele respective vor fi transmise către terți;
- s) După caz, în alte scopuri stabilite de legislația în vigoare.

2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență contabilă în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență contabilă din cadrul Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău se prelucrează/stochează:

- 1. pe suport de hîrtie;
- 2. în format electronic:
 - a) Software – Sistemul de evidență contabilă 1C, versiunea 8, care este instalat la 7 computatoare din cadrul Secției rapoarte financiare și evidență contabilă aflîndu-se în biroul Nr.5 în sediul Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău ;
 - b) Software – Sistemul de evidență contabilă “Salariu”, care este instalat la 3 computatoare din cadrul Secției rapoarte financiare și evidență contabilă aflîndu-se în biroul Nr.5 în sediul Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău;
 - c) Software – utilizarea sistemelor on-line cum ar fi: SIA E-REPORTING, E-alocație, E-doplă și alte prevăzute de legislație în vigoare.

d) Hardware :

- calculator nr de inventariere - 31460052 posedă: 1C, "Salariu", SIA E-reporting E-alocații, E-docplat;
- calculator nr de inventariere – 31460103 posedă: 1C, SIA E-reporting E-alocații, E-docplat;
- calculator nr de inventariere - 31460110 posedă : 1C, "Salariu";
- calculator nr de inventariere - 31460049 posedă: 1C, "Salariu";
- calculator nr de inventariere - 31460054 posedă: 1C;
- calculator nr de inventariere - 31460051 posedă: 1C;
- calculator nr de inventariere - 31460111 posedă: 1C;

3.2. Mentenanța programului contabil 1C este efectuată de către compania „InfoSoftTeh” SRL, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între Direcția generală asistență socială și sănătate a Consiliului municipal Chișinău și compania InfoSoftTeh” SRL, cu următoarele atribuții stabilite companiei prestatoare:

- Efectuarea ajustărilor în programul contabil "1C", în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului contabil "1C" ;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului contabil "1C" (Linia fierbinte);
- Examinarea solicitărilor parvenite din partea Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău cu privire la utilizarea programului contabil "1C" ;
- ;
- Examinarea bazei de date a Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău (la necesitate) ;
- Vizite la fața locului, la solicitarea Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău;
- Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

3.3. Mentenanța programului contabil „Salariu” este efectuată de către persoana fizică dl. Botnarenco Sergiu, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între Direcția asistență socială și sănătate a Consiliului municipal Chișinău și persoana fizică dl. Botnarenco Sergiu, cu următoarele atribuții stabilite companiei prestatoare:

- Strămutarea lunară a bazei de date din programul contabil „Salariu” în programul contabil "1C", ambele programe aparținând Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău;
- Eliminarea erorilor în funcționarea programului;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului contabil „Salariu” ;
- Examinarea solicitărilor parvenite din partea Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău cu privire la utilizarea programului contabil „Salariu” ;

3.4. Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hârtie este structurată după criteriul "măpe-dosare", fiind păstrate în dulapuri, care sînt amplasate fizic în biroul Nr. 5 din sediul Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău.

III. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează pe perioada valabilității contractelor de achiziție publică, pe perioada activității angajaților Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău (din momentul semnării contractului pînă la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență contabilă sînt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență contabilă vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțămîntul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ

6.1. Măsurile generale de administrare a securității informaționale

6.1.1. În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronic care conțin date preluate din sistemul de evidență contabilă, aceștia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.

6.1.3. Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.

- 6.1.4. Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență contabilă este blocat împotriva vizualizării de către persoane neautorizate.
- 6.1.5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență contabilă sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
- 6.1.6. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență contabilă din/în perimetrul de securitate se înregistrează în registru.
- 6.2. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență contabilă, se înfăptuiesc ținînd cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică.
- 6.3. Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență contabilă, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.
- 6.4. Accesul în biroul unde este amplasat sistemul de evidență contabilă este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.
- 6.5. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.
- 6.6. Înainte de acordarea accesului fizic la sistemul de evidență contabilă, se verifică competențele de acces.
- 6.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.
- 6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență contabilă, fiind integru din punct de vedere fizic.
- 6.9. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență contabilă, din punct de vedere fizic.
- 6.10. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.
- 6.11. Ușile și ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.
- 6.12. Amplasarea sistemului de evidență contabilă răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- 6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență contabilă, 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 de evidență contabilă, inclusiv posibilitatea deconectării oricărui component TI.
- 6.14. Computerele, unde este amplasat fizic sistemul de evidență contabilă, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.
- 6.15. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență contabilă, sînt protejate contra conectărilor

nesanționate sau deteriorărilor. Pentru a exclude bruiatul, cablurile de tensiune sînt separate de cele comunicaționale.

6.16. Securitatea antiincendiară a sistemului de evidență contabilă: biroul unde este amplasat sistemul de evidență contabilă este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiară în vigoare.

6.17. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemului de evidență contabilă. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

VII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ CONTABILĂ

7.1. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din sistemele de evidență contabilă și a proceselor executate în numele acestor utilizatori.

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

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lîngă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 /un/ an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare și autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont

de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 /una/ lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din sistemul de evidență contabilă. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

7.9. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieste cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidență contabilă.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privința persoanelor care au dreptul:

- a) să vizualizeze informațiile stocate în sistemul de evidență contabilă;
- b) să copieze, să descarce, să șteargă sau să modifice orice informație stocată.

7.12. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securității în ceea ce privește sistemul de evidență contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemului de evidență contabilă este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ CONTABILĂ

8.1. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență contabilă pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

8.2. 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.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemele de evidență contabilă, 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 al procesului;
- c) ID-ul utilizatorului;
- d) rezultatul tentativei de pornire – pozitivă sau negativă.

8.4. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul de evidență contabilă, conform următorilor parametri:

- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
- b) denumirea (identificatorul) aplicației sau a 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.

8.5. Se efectuează 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.

8.6. Se efectuează înregistrarea ieșirii din sistemul de evidență contabilă, 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, filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securității în sistemul de evidență contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

8.8. Rezultatele auditului securității în sistemul de evidență contabilă (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

8.9. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență contabilă constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a 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 INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență contabilă, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestora, protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

9.2. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul de evidență contabilă.

9.3. Se asigură testarea funcționării corecte a componentelor de securitate a sistemului de evidență contabilă (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență contabilă și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidență contabilă trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență contabilă.

10.3. În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

10.4. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență contabilă poartă răspundere civilă, contravențională și penală.

XI. DISPOZIȚII FINALE

11.1. Prezentul Regulament este revizuit și ulterior aprobat de către conducerea Direcției generale asistență socială și sănătate a Consiliului municipal Chișinău periodic, însă cel puțin o dată în an, precum și la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

11.3. Regulamentul este adus la cunoștința angajaților contra semnăturii.

11.4. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.