CONSILIUL NAȚIONAL PENTRU DETERMINAREA DIZABILITĂȚII ȘI CAPACITĂȚII DE MUNCĂ

ORDIN Nr. 147
din 04.11.2019

„Cu privire la aprobarea Regulamentului Securității Informaționale a Consiliului Național pentru Determinarea Dezabilității și Capacității de Muncă"

În conformitate cu prevederile Regulamentului privind organizarea şi funcţionarea Consiliului Naţional pentru Determinarea Dizabilităţii şi Capacităţii de Muncă aprobat prin Hotărârea Guvernului nr. 357 din 18 aprilie 2018 cu privire la determinarea dizabilităţii",

ORDON:

I. Se aprobă Regulamentul Securității Informaționale a Consiliului Național pentru Determinarea Dezabilității și Capacității de Muncă.

II. Se desemnează dra Emilia Berejnaia, Șef serviciu tehnologii informaționale și monitorizare, persoană responsabilă de monitorizarea, înregistrarea incidenteleor în domeniul securităţii informaţionale în cadrul Consiliului, inclusiv completarea și gestionarea Registrului electronic al incidentelor în domeniul securităţii informaţionale.

III. Serviciul tehnologii informaționale și monitorizare va înregistra toate echipamentele conform cerințelor impuse prin prezentul Regulament, precum și cererile de conectare la echipament în Registrul electronic al echipamentelor.

IV. Responsabil de lista utilizatorilor în SIAAS este șef Serviciu tehnologii informaționale și monitorizare.

V. Responsabil de semnarea Acordului de confidențialitate a utilizatorului Sistemului de Informații privind confidențialitatea datelor cu caracter personal și Declarația – angajament a utilizatorului SIAAS privind confidențialitatea datelor cu caracter personal este șef Serviciul resurse umane, informare și comunicare.

VI. Serviciul tehnologii informaționale și monitorizare va informa toți colaboratorii Consiliului, despre Regulamentul sus menționat.

VII. Controlul asupra executării prezentului ordin mi-l asum.

Director N. Mamaliga **Narcisa MAMALIGA**

Am luat cunoştinţă Berejnaia Emilia Berejnaia
Am luat cunoştinţă O. Ciobanu Oxana Ciobanu

Aprobat
prin Ordinul directorului
nr. 44 din 04.12.2015

REGULAMENTUL

Securităţii Informaţionale a Consiliului Naţional pentru Determinarea Dezabilităţii şi Capacităţii de Muncă

CAPITOLUL I
1. INFORMAŢII GENERALE

1.1 Regulamentul Securităţii Informaţionale (în continuare - *Regulament*) stabileşte măsurile de protecţie şi de securitate a informaţiilor utilizate, stocate, transmise sau prelucrate de către Consiliului Naţional pentru Determinarea Dizabilităţii şi Capacităţii de Muncă (în continuare - *Consiliu*) şi structurile sale în Sistemul Informaţional Automatizat „Asistenţă Socială" (în continuare – *SIAAS*).

1.2 În sensul prezentului Regulament următoarele noţiuni semnifică:

- *utilizator* – persoană cu drept de acces, deplin sau partajat, asupra informaţiei din resursa informaţională;
- *informaţie* – totalitate a datelor materializate pe suport de hîrtie sau generate electronic cu referire la un dosar, din momentul înregistrării cererii de determinare a gradului de dizabilitate pînă la emiterea deciziei definitive şi transmiterea lui arhivă;
- *gestionare electronică a dosarelor* – totalitate a acţiunilor legate de administrarea dosarelor prin intermediul platformei electronice sau a sistemului informaţional automatizate;
- *prelucrare automatizată de date* – orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor prin mijloace automatizate, precum: colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;
- *securitate* – nivel necesar de integritate, selectivitate pentru protejarea datelor împotriva pierderilor, alterărilor, deteriorărilor şi a accesului neautorizat. Securitatea sistemului presupune faptul că acesta este rezistent la atacuri, informaţia este confidenţială, integrală şi în stare de lucru, atît la nivel de sistem, cît şi la nivel de date;
- *sistem informaţiona l*– sistem informaţional automatizat constituit dintr-un ansamblu de resurse şi tehnologii informaţionale, mijloace tehnice de program şi metodologii aflate în interconexiune şi care este destinat înregistrării, prelucrării, utilizării, păstrării,

informaţiilor cu privire determinarea dizabilităţii din momentul înregistrării acestora pînă în momentul arhivării;

- *date personale* - date despre o persoană fizică ce permit identificarea ei directă sau indirectă;
- *date cu caracter personal* – orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal).

CAPITOLUL II.
2. ORGANIZAREA SECURITĂŢII INFORMAŢIONALE INTERNE

2.1 Organizarea securităţii informaţiei se efectuează de către conducerea Consiliului privind securitatea informaţiei. În cazul în care conducerea Consiliului nu are specialişti în domeniu, aceasta poate apela pentru consultanţă la specialişti calificaţi.

2.2 Intrările de informaţii sau servicii oferite de părţile externe nu trebuie să influenţeze gradul de securitate al informaţiilor. Accesul părţilor externe la mijloacele de prelucrare a datelor (software şi hardware), precum şi prelucrarea şi transmiterea informaţiei părţilor externe trebuie să fie monitorizate. Relaţiile cu părţile externe care solicită acces la informaţii din cadrul Sistemului Informaţional şi prelucrarea lor sunt supuse analizei riscurilor.

2.3 Angajamentul Consiliului privind securitatea informaţiei. Consiliul va asigura:

2.3.1 Identificarea obiectivelor în domeniul securităţii informaţionale, care satisfac cerinţele organizatorice, va formula, examina şi aproba reguli şi instrucţiuni privind securitatea informaţiei;

2.3.2 Examinarea impactului punerii în aplicare a politicii, regulamentelor şi procedurilor de protecţie a informaţiei;

2.3.3 Întocmirea regulilor clare şi aprobarea lor de către conducerea Consiliului în privinţa securităţii informaţiei;

2.3.4 Identificarea resurselor tehnologice şi financiare necesare pentru implementarea politicii securităţii informaţiei;

2.3.5 Aprobarea rolurilor şi responsabilităţilor specifice pentru protecţia informaţiei în cadrul Consiliului;

2.3.6 Iniţierea planurilor şi programelor pentru asigurarea unui grad înalt de conştientizare a securităţii informaţiei;

2.3.7 Identificarea, coordonarea şi punerea în aplicare a controalelor de securitatea a informaţiei.

2.4 Coordonarea securităţii informaţiei.

a) Toate acţiunile privind securitatea informaţiei trebuie să fie coordonate cu organul ierarhic superior.
b) În procesul de coordonare a securităţii informaţionale participă angajaţi ai Consiliului.

2.5 Alocarea responsabilităţilor pentru securitatea informaţiei.

2.5.1 Conducerea Consiliului este responsabilă pentru politica de securitate a informaţiei şi trebuie să asigure resursele necesare pentru combaterea ameninţărilor vis-a-vis de activitatea sa.

2.5.2 Şef Serviciu tehnologii informaţionale şi monitorizare asigură monitorizarea respectării de către toţi utilizatorii a cerinţelor prevăzute prezentul Regulamen, gestionează eliberarea sau anularea acceselor la SIAAS, colectează cererile parvenite de la utilizatori şi execută cererile aprobate de conducerea Consiliului, monitorizează executarea lucrărilor aferente securităţii informaţiilor.

2.5.3 Şefii subdiviziunilor (Şefii de secţii, servicii, birou) se asigură că personalul din subordine sunt pe deplin conştienţi de politica, regulamentele şi procedurile de securitate a informaţiei şi nu realizează obiective care sunt în contradicţie cu prevederile politicii, regulamentelor şi procedurilor. Ei asigură aplicarea politicii şi verifică progresul privind implementarea acestei politici.

2.5.4 Utilizatorii sunt responsabili pentru acţiunile lor. Ei sunt conştienţi de politica de securitate a Consiliului, înţeleg care sunt consecinţele acţiunilor lor şi acţionează în conformitate cu reglementările în vigoare. Ei au la dispoziţie mecanisme eficiente, astfel încât să poată opera la nivelul dorit de securitate.

2.6 Procesul de autorizare pentru sistemele de procesare a informaţiei.

2.6.1 Accesul la staţiile de lucru şi la sistemul de operare se efectuează strict la nivel limitat (nivel utilizator) prin autentificare cu parola personală.

2.6.2 Este interzisă conectarea echipamentelor la reţeaua de comunicaţii a CNDDCM care nu se afla în gestiunea CNDDCM.

2.6.3 Conectarea echipamentelor care nu aparţin CNDDCM la reţeaua de comunicaţii se efectuează în cazurile când:

- Echipamentele personale ale utilizatorilor în cazuri de necesitate de serviciu;
- Echipamentele reprezentanţilor organizaţiilor internaţionale care îndeplinesc atribuţiile de serviciu în baza acordurilor internaţionale şi bilaterale;
- Alte cazuri acceptate de conducerea Consiliului.

2.6.4 Conectarea echipamentelor trebuie sa urmeze următorii paşi:

- Solicitantul trebuie să depună cerere în forma scrisă pentru conectare utilajului în reţea pe numele Şefului serviciului tehnologii informaţionale şi monitorizare.
- Pentru cazurile de conectare a echipamentelor în baza contractelor internaţionale şi bilaterale conducerii Consiliului primeşte decizia respectivă.
- Conectarea echipamentului va fi fixată de către administratorul de sistem în registrul electronic al echipamentelor.
- Solicitarea va fi păstrată de către administratorul de sisteme informaţionale în mapa „Solicitări".

2.6.5 Modificarea setărilor staţiilor de lucru poate fi efectuată doar de către personalul Serviciului tehnologii informaţionale şi monitorizare.

2.7 Acorduri de confidenţialitate.

2.7.1 Informaţiile gestionate în SI au caracter confidenţial şi pot fi distribuite strict conform legislaţiei în vigoare.

2.7.2 Pentru admiterea accesului la resurse informaţionale protejate ale SI sunt admişi doar colaboratori cu care este semnat Acordul de confidenţialitate a utilizatorului Sistemului de Informaţii privind confidenţialitatea datelor cu caracter personal şi Declaraţia – angajament a utilizatorului Sistemului Informaţional Automatizat Asistenţa Socială (SIAAS) privind confidenţialitatea datelor cu caracter personal care se păstrează în dosarul personal al colaboratorului.

2.7.3 Accesul la resursele informaţionale protejate ale Sistemului informaţional este permis doar colaboratorilor care au semnat Declaraţia de familiarizare cu regulamentul în cauza. Declaraţia se păstrează în dosarul personal al colaboratorului la Serviciul resurse umane, informare şi comunicare.

2.8 Soluţionarea scurgerii informaţiei din Sistemul informaţional (în continuare – *SI*).

2.8.1 Cazul depistării scurgerii de informaţie din cadrul SI, persoana care a depistat scurgerea informaţiei este obligat imediat să informeze Administratorul sisteme informaţionale;

2.8.2 Administratorul SI organizează lucrările necesare pentru a bloca sursa de scurgere a informaţiei.

2.8.3 Administratorul SI raportează în formă scrisă conducerii Consiliului cauza scurgerii informaţiei şi acţiunile întreprinse.

2.8.4 Administratorul SI în comun cu administratorii SIAAS elaborează şi implementează măsuri pentru neadmiterea cazurilor de scurgere a informaţiei.

2.8.5 În cazul depistării factorului uman implicat în scurgerea informaţiei administratorul SI informează conducerea Consiliului pentru întreprinderea măsurilor în conformitate cu legislaţia în vigoare.

2.9 Auditul SIAAS privind protecţia securităţii informaţionale.

În caz de necesitate sau lipsei specialiştilor certificaţi în cadrul Secţiei tehnologii informaţionale şi monitorizare, conducerea Consiliului poate solicita auditul securităţii informaţiei a SIAAS de la organizaţii externe.

CAPITOLUL III
SECURITATEA RESURSELOR UMANE ÎNAINTEA ANGAJĂRII

3.1 Roluri şi responsabilităţi. Rolurile şi responsabilităţile angajaţilor, contractanţilor şi utilizatorilor terţi privind securitatea informaţiei sunt clar definite şi documentate în procedura stabilită de către Serviciul resurse umane, informare şi comunicare.

3.2 Verificare angajaţilor. Pentru toţi candidaţii pentru angajare, contractanţii şi trebuie să se efectueze controale de verificare de fond în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu cerinţele activităţii, clasificarea informaţiei la care urmează să aibă acces şi riscurile percepute.

3.3 Candidaţii care pretind să fie încadraţi permanent sau temporar sunt verificaţi din momentul depunerii cererii. Verificarea cuprinde următoarele proceduri:

a) existenţa recomandărilor pozitive, în special în ceea ce priveşte calităţilor profesionale şi calităţile personale ale solicitantului;
b) verificarea corespunderii datelor din CV-ul solicitantului;
c) confirmarea calificărilor personale şi profesionale;
d) cerficarea independentă a autenticităţii documentelor de identitate.

3.4 Acordul de confidenţialitate.

3.4.1 Acordul de confidenţialitate este folosit pentru a notifica angajaţii că informaţiile pe care o gestionează sunt confidenţiale sau secrete. Angajaţi, semnează Acordul ca parte integrantă a contractului de muncă. Acordul de confidenţialitate se păstrează în dosarul personal al angajatului, conform procedurii stabilite. Formularul acordului de confidenţialitate este elaborat de către Serviciul resurse umane, informare şi comunicare.

3.4.2 Angajaţii temporari, experţii, şi reprezentanţi ai unor părţi terţe care nu activează în conformitate cu contractul individual de muncă standard (care conţine un acord de confidenţialitate) semnează acorduri separate de confidenţialitate înainte de a li se acorda acces la SI.

3.4.3 Acordul de confidenţialitate este revizuit în cazul în care are loc modificarea contractului individual de muncă, în special în cazul unei schimbări a drepturilor angajatului sau expirarea contractelor individuale de muncă.

3.5 Contractul de muncă.

Contractul individual de muncă identifică angajatul responsabil pentru securitatea informaţiei. În cazul în care este necesar, această responsabilitate trebuie să fie menţinută şi pentru o anumită perioadă după încetarea contractului. Divulgarea

informaţiei confidenţiale sau secrete la care are sau a avut acces angajatul se sancţionează conform legislaţiei în vigoare.

3.6 Cerinţe şi condiţii de angajare.

Ca parte a obligaţiilor contractuale, angajaţii, contractanţii şi utilizatorii sunt obligaţi să semneze cerinţele şi condiţiile contractului de angajare, care trebuie să precizeze responsabilităţile lor şi ale organizaţiei pentru securitatea informaţiei.

4. ÎN TIMPUL PERIOADEI DE ANGAJARE

4.1 Responsabilităţile managementului.

4.1.1. Şefii subdiviziunilor Consiliului cer angajaţilor, contractanţilor şi utilizatorilor terţi să aplice măsurile de securitate în conformitate cu politica, regulamentele şi procedurile stabilite de către Consiliu.

4.1.2. Şefii subdiviziunilor Consiliului evaluează nivelul adecvat de supraveghere a personalului neexperimentat, cărora li sa acordat dreptul de acces la informaţia sensibilă. Procedurile de monitorizare periodică şi aprobarea acţiunilor tuturor angajaţilor de către superiorii se fac continuu.

4.1.3. Şefii subdiviziunilor Consiliului sunt conştienţi de faptul că problemele personale ale angajaţilor pot afecta activitatea acestora. Problemele personale sau financiare ale angajaţilor, modificările de comportament sau stil de viaţă, semnele de stres sau depresie, pot fi o cauza de fraudă, furt, erori sau alte încălcări ale securităţii. Aceste informaţii sunt luate în considerare în conformitate cu legislaţia în vigoare.

4.1.4. Şefii subdiviziunilor Consiliului au dreptul să solicite informaţia referitor la utilizatorii care activează în raza subdiviziunilor pentru a reverifica listele utilizatorilor activi.

4.1.5. Conducătorii subdiviziunilor duc responsabilitate pentru:

a) aducerea la cunoştinţă utilizatorilor subdiviziunilor sale toate reglementările privind securitatea informaţiei sub semnătura personală;

b) îndeplinirea cerinţelor privind protecţia colaboratorilor subdiviziunilor sale în lucrul cu SIAAS;

c) eliberarea la timp a cererilor privind modificarea înscrierilor de evidenţă ale colaboratorilor subdiviziunilor sale şi asigurarea lor cu drepturi de acces, strict în limitele necesare îndeplinirii sarcinilor sale de serviciu;

d) informare imediată a specialiştilor din cadrul Consiliului despre descoperirea faptului încălcării securităţii informaţiei în sistemele informaţionale;

e) luarea tuturor măsurilor necesare pentru lichidarea consecinţelor încălcării securităţii informaţiei;

f) asigurarea controlului permanent privind respectarea cerinţelor prezentului Regulament.

CAPITOLUL IV.
SECURITATEA FIZICĂ ŞI A MEDIULUI DE LUCRU

5. DISPOZIŢII GENERALE

5.1 Mijloacele de prelucrare a informaţiilor critice sau sensibile trebuie să fie situate în zone de securitate, care sunt protejate de anumite perimetre de securitate, cu bariere de siguranţă şi de control de acces corespunzător.

5.2 Acestea trebuie să fie protejate fizic împotriva accesului neautorizat, daune şi interferenţe.

5.3 Protecţia oferită trebuie să fie proporţională cu riscurile identificate.

5.4 Echipamentele trebuie să fie protejate împotriva ameninţărilor fizice şi de mediu.

5.5 Protecţia echipamentelor (inclusiv echipamentele folosite în afară locului de muncă şi scoaterea în afara sediilor) este necesar pentru a reduce riscul de acces neautorizat la informaţii şi protejarea împotriva pierderii sau deteriorării.

6. ZONE DE SECURITATE

6.1 Perimetrul fizic de securitate

Pentru a proteja zonele care conţin informaţii şi sisteme de procesare a informaţiei trebuie folosită perimetrea de securitate (bariere precum pereţi, porţi de acces controlat pe baza de card sau birouri de recepţie cu personal de securitate).

6.2 Controlul accesului fizic

6.2.1 Zonele de securitate trebuie protejate prin controale adecvate ale accesului fizic pentru a se asigura că accesul este permis doar personalului autorizat.

6.2.2 Accesul fizic la toate încăperile unde este instalat echipament trebuie să fie documentate şi protejate;

6.2.3 Este asigurat cu sistem de control al accesului, identificarea fiind înfăptuită prin cârd.

6.2.4 Este asigurat cu sistem de supraveghere video, care permite monitorizarea în interior.

6.2.5 Înregistrările video din sistemul de monitorizare trebuie arhivate timp de cel puţin trei luni.

6.2.6 Rata de cadre a sistemului de monitorizare trebuie să fie de cel puţin 7 fps (cadre pe secundă).

6.2.7 Acces are strict personalul Secţiei tehnologii informaţionale şi monitorizare.

6.3. Securizarea birourilor, încăperilor şi a sistemelor informaţionale

6.3.1. Consiliul trebuie să proiecteze şi să implementeze măsuri pentru securizarea fizică a birourilor, încăperilor şi a sistemelor informaţionale.

6.3.2. Pentru protejarea oficiilor, birourilor şi a echipamentelor trebuie respectate normele şi standarde tehnicii de securitate şi securitate a muncii;

6.3.3. Activele cheie trebui să fie amplasate astfel încât să se evite accesul publicului larg;

6.3.4. Indicatoarele care reflectă dislocarea zonelor de securitate nu trebuie să fie uşor accesibile publicului larg;

6.4.Protejarea împotriva ameninţărilor externe şi de mediu;

6.4.1. Consiliul trebuie să proiecteze şi să aplice măsuri de protecţie fizică împotriva incendiilor, inundaţiilor, cutremurelor, exploziilor, revoltelor publice şi a oricăror alte forme de dezastre naturale sau produse de oameni;

6.4.2. Materiale periculoase sau inflamabile trebuie să fie depozitate la o distanţă sigură din zona de siguranţă. Produse de papetărie şi birotică nu trebui să fie păstrate în zonele de securitate;

6.4.3. Copiile de rezervă şi de back-up trebuie să fie amplasate la o distanţă de siguranţă pentru a evita deteriorarea lor;

6.4.4. Asigurarea cu sistem antiincendiar adecvat, cu detectoare fum, căldură, sistem de stingere cu gaz, sistem de ventilare. Este instalată uşa ignifugă şi au fost utiliza materiale rezistente la foc pentru pereţi şi tavan.

6.5 Desfăşurarea activităţii în zone de securitate

6.5.1. Consiliul trebuie să proiecteze şi să aplice măsuri şi ghiduri pentru protecţia fizică şi pentru desfăşurarea activităţii în zone de securitate.

6.5.2. Personalul trebuie să fie informat despre existenţa zonelor de securitate sau activitatea în zona de securitate - strict după necesităţi de serviciu;

6.5.3. Trebui să fie evitate activităţile nesupravegheată în zone de securitate, din considerente de securitate precum şi prevenirea acţiunilor răuvoitoare ;

6.5.4. Zonele de securitate neutilizate trebuie să fie fizic blocate şi periodic blocate

6.5.5. Se interzice introducerea echipamentului de înregistrare audio, foto, video în zonele de securitate;

6.6 Zone de acces public, punctele de livrare şi încărcare

6.6.1. Punctele de acces precum punctele de livrare şi încărcare sau alte puncte pe unde persoanele care nu sunt autorizate pot intra în interior trebuie controlate şi, dacă este posibil, izolate de sistemele de procesare a informaţiei pentru a se evita accesul neautorizat.

7. SECURITATEA ECHIPAMENTELOR

7.1 Amplasarea şi protejarea echipamentelor

7.1.1 Echipamentele trebuie să fie amplasate şi protejate astfel încât să se reducă riscurile faţă de ameninţările şi pericolele de mediu şi faţă de posibilitatea de acces neautorizat.

7.1.2 În scopul de a proteja echipamentele, trebuie să fie luate în considerare următoarele:

a) Echipamentele trebuie să fie amplasate astfel încît să minimizeze accesul în zonele de securitate;

b) Elemente care necesită o protecţie specială ar trebui să fie izolate, în vederea reducerii nivelului general de protecţie;

c) Trebuie să fie stabilite controale pentru a minimiza riscul posibilelor ameninţări fizice, cum ar fi furt, incendiu, agenţi explozibili, fum, apă (sau eşecul în furnizarea de apă), praf, vibraţii, agenţi chimici, penelor de curent electric, interferenţe de comunicare, electromagnetice, radiaţii şi vandalism;

d) Se interzice consumul alimentar şi de băuturi, fumatul în apropierea zonelor de securitate;

e) Condiţiile de mediu, cum ar fi temperatura şi umiditatea trebuie să fie continuu monitorizate pentru condiţii care ar putea influenţa negativ asupra mijloacelor de prelucrare a informaţiei;

f) Protecţie la trăsnet ar trebui să fie aplicate la toate clădirile şi filtre antitrăsnet trebuie să fie instalate pe toate liniile de tensiune şi linii de comunicaţii;

g) Mijloacele care gestionează informaţii sensibile trebuie să fie protejate în scopul de a reduce la minimum riscul scurgerii de informaţii prin intermediul iradierilor colaterale.

7.2 Utilităţile suport pentru afacere

7.2.1 Echipamentele trebuie să fie protejate împotriva penelor de curent sau a altor întreruperi cauzate de problem ale utilităţilor suport.

7.2.2 Toate utilităţile de sprijin, cum ar fi electricitate, apă, canalizare, încălzire /ventilaţie şi aer condiţionat trebui să fie adecvate sistemelor ce le deservesc, monitorizate în mod regulat şi, după caz, să fie testate.

7.2.3 Toate echipamentele care prelucrează informaţie sensibilă, trebuie să fie conectate la reţeaua electrică prin surse de alimentare de rezervă (UPS).

7.2.4 Echipamentele de telecomunicaţii sunt conectate la 2 furnizori, pentru a asigura funcţionare continuă a conexiunilor.

7.3 Securitatea reţelelor de cablu

7.3.1 Cablurile de energie şi reţelele de telecomunicaţii purtătoare de date sau servicii de suport pentru informaţie trebuie protejate faţă de interceptări sau avarii.

7.3.2 Pentru asigurarea securităţii cablurilor de energie sau comunicaţie trebuie să se îndeplinească următoarele:

a) Informaţiile transmise prin reţelele de telecomunicaţii sunt protejate de către proprietarul echipamentului (Moldetelecom, CTS, etc.);

b) Proprietarul reţelelor de cablu asigură o securitate corespunzătoare, ţinînd cont de riscurilor de avariere;

c) Acest lucru în mod obligatoriu trebuie să fie stipulat în contractul de prestare a serviciilor;

d) Cablurile şi echipamentele trebuie să fie marcate pentru a evita erorile de manipulare greşită, ca conexiunea incorectă de cabluri;

e) Pentru a evita posibile erori, conexiunile trebuie să fie documentate;

7.3.3 Reţelele de cablu ce deservesc sistemele informaţionale importante trebuie să fie asigurate cu:

a) Canale armate şi camere blocate sau panouri în locurile de control şi locurile conexiune;

b) Utilizarea rutărilor alternative;

c) Utilizarea cablurilor optice;

d) Utilizarea ecranelor electromagnetice;

e) Controlul accesului la panourile de comunicaţii.

7.4 Întreţinerea echipamentelor

7.4.1 Echipamentele trebuie să fie corect întreţinute pentru a se asigura disponibilitatea continuă şi integritatea acestora.

7.4.2 La întreţinerea echipamentului trebuie să se ia în considerare următoarele:

a) Echipamentele trebuie să fie întreţinute conform recomandărilor producătorului cu periodicitatea şi specificările descrise în documentele tehnice.

b) Întreţinerea se efectuează strict de către persoanele autorizate.

c) Să se efectueze o strictă evidenţă a tuturor defectelor presupuse sau reale, precum şi deservirii de profilactică şi de reparare.

d) Dacă echipamentul este inclus într-un grafic de deservire trebuie să fie luat în considerare de cine este efectuată deservirea, personal interior sau din exterior, şi daca este necesar din echipament trebuie eliminată informaţia de serviciu.

e) Cerinţele impuse de poliţele de asigurare trebuie să fie respectate.

7.5 Securitatea echipamentului în afara locaţiei

7.5.1 Pentru echipamentele scoase în afara locaţiei trebuie să fie asigurată o securitate corespunzătoare, ţinându-se cont de riscurile diferite pentru activităţile care se desfăşoară în afara locaţiei.

7.5.2 Echipamente şi purtătorii de informaţii care sunt scoase în afara sediilor nu pot fi lăsate nesupravegheate în locuri publice, atunci când călătoresc trebuie să fie transportate ca bagaje de mână şi trebuie să fie mascate, dacă este posibil şi apărate de influenţe electromagnetice;

7.5.3 Securitatea echipamentului din în afara locaţiei, utilizat de către Consiliu, este asigurat de către proprietarul echipamentului (Moldtelecom, CTS, etc.). Proprietarul echipamentului asigură o securitate corespunzătoare, ţinînd cont de riscurile pentru activităţile care se desfăşoară în afara locaţiei. Acest lucru în mod obligatoriu trebuie să fie stipulat în contractul de prestare a serviciilor.

7.6 Scoaterea din uz sau reutilizarea în condiţii de siguranţă

7.6.1 Toate părţile din echipament care conţin medii de stocare sunt verificate pentru a se asigura că orice date importante sau produse software licenţiat a fost înlăturat sau suprascris într-un mod sigur înainte de distrugere.

7.6.2 Echipamentele care conţin informaţii confidenţiale trebuie să fie fizic distruse sau informaţiile trebuie să fie distruse sau eliminate folosind tehnici pentru a face informaţia originală nerecuperabilă.

CAPITOLUL V.
MANAGEMENTUL COMUNICAŢIILOR ŞI OPERAŢIUNILOR
8. PROCEDURI OPERAŢIONALE ŞI RESPONSABILITĂŢI

8.1 Documentarea procedurilor de operare.

Toate procedurile de operare trebuie să fie documentate, păstrate şi puse la dispoziţia tuturor celor care au nevoie de ele. Persoana responsabilă de documentare este nominalizată de către conducerea Consiliului.

8.2 Prin intermediul responsabilului SI se asigură accesul la documentaţia tehnică relevantă utilizatorilor SIAAS, conform atribuţiilor de serviciu.

9. SCHIMBUL DE INFORMAŢII

9.1 Proceduri şi politici pentru schimbul de informaţii. Schimbul de informaţii între Consiliu şi autoritatea externă poate fi efectuat numai în baza acordurilor bilaterale de schimb date;

9.2 Acordurile bilaterale obligatoriu trebuie să conţină următoarele informaţii - lista datelor la care se solicită acces; lista persoanelor care vor avea acces;

9.3 Pentru asigurarea schimbului de date obligatoriu se utilizează servere intermediare;

9.4 Schimbul de date se efectuează numai prin intermediul reţelelor de comunicaţii protejate.

CAPITOLUL V.
10. MONITORIZAREA

10.1 Jurnal de audit. Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale SIAAS.

10.2 Monitorizarea utilizării sistemului

10.2.1 Nu mai rar de odată în trei luni administratorii de sisteme vor efectuata evaluarea riscurilor pentru resursele importante din Lista resurselor TI ale Consiliului pentru a preveni eventualele situaţii de înrăutăţire a performanţelor.

10.2.2 Toate resursele TI ale Consiliului importante sunt monitorizate de către administratorii SIAAS, pentru a anticipa devierile în funcţionare conform normelor recomandate;

10.2.3. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:

a) Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;

b) Tipul traficului în reţea, a protocoalelor şi a echipamentelor conectate la SIAAS, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;

c) Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

10.2.4 În mod regulat (cel puţin o dată în trei luni) de administratorii SIAAS se vor efectua verificări, pentru detectarea:

a) Parolelor utilizator care nu respectă regulamentele;
b) Echipamentelor de reţea conectate neautorizat;
c) Serviciilor de reţea neautorizate;
d) Serverilor de pagini de web neautorizate;
e) Echipamentelor ce utilizează resurse comune nesecurizate;
f) Utilizării de modeme neautorizate;
g) Licenţelor pentru sistemele de operare şi programele instalate;

10.2.5 În cazul depistării oricărei nereguli în rezultatul evaluărilor descrise în punctul 7.1, administratorul baze de date a Secţiei tehnologii informaţionale și monoitorizare este obligat:

a) Să descrie în raport către şeful Secţiei riscul depistat.

b) Să estimeze consecinţele care pot apărea în SIAAS în urma nesoluţionării problemei care a cauzat riscul.

c) Să identifice metodele de soluţionare pentru excluderea riscurilor identificate.

d) Şeful secţiei raportează conducerii Consiliului despre riscul identificat şi modalitatea de soluţionare a acestuia.

e) Şeful secţiei ia toate măsurile necesare pentru excluderea riscului identificat.

10.2.6. în cazul în care pentru excluderea riscului sunt necesare cheltuieli financiare suplimentarea, şeful Secţiei tehnologii informaţionale şi monoitorizare trebuie:

a) Să pregătească divizul de cheltuieli pentru soluţionarea riscului.

b) Să gestioneze procedura de implementare a soluţiei.

10.3 Protecţia informaţiilor din jurnale.

10.3.1. Jurnalele de audit descrise în punctul 10.1 periodic se vor arhiva şi se vor păstra conform actelor normative.

10.3.2. Responsabil pentru arhivarea şi păstrarea fişierelor jurnal este administratorul de sistem.

10.4. Jurnalul activităţilor administratorului şi operatorului.

Activităţile administratorului de sistem şi ale operatorului de sistem trebuie înregistrate.

10.5. Înregistrarea erorilor şi deficienţelor în funcţionare.

10.5.1. Incidentelor securităţii informaţionale li se atribuie următoarele evenimente:

a) pierderea serviciilor prestate, lipsa funcţionării continuă a echipamentelor şi mijloacelor de prelucrare şi transmitere a informaţiilor;

b) erori de sistem sau a supraîncărcării resurselor de prelucrare şi transmitere a informaţiei;

c) erori a utilizatorilor şi a personalului TI;

d) întreruperi în SIAAS, cauzate de nerespectarea recomandărilor actelor normative şi nomelor securităţii informaţionale;

e) întreruperi şi nefuncţionarea resurselor de prelucrare şi transmitere a informaţiei;

f) modificări necontrolate în sistemele de prelucrare şi transmitere a informaţiei;

g) încălcarea regulilor de acces în perimetru de securitate a Consiliului;

h) atacurile viruşilor, atacuri cibernetice şi infracţiuni, acces extern nesancţionat sau transmiterea datelor în/din SIAAS;

i) încălcarea integrităţii, accesibilităţii, confidenţialităţii, responsabilităţii, autenticităţii informaţiilor;

10.5.2. De asemenea, incidentelor li se atribuie evenimentele, care pot apărea:

a) în sistemul de alimentare cu energie electrică în centru de prelucrare a datelor;

b) în sistemul de alimentare cu energie electrică a subdiviziunilor Consiliului;

c) în reţele locale (LAN, WAN) şi la echipamente;

d) la computerele personale de la locul de muncă a utilizatorilor şi la alte echipamente şi tehnologii;

e) în centru de prelucrare a datelor;

f) în sistemul administrării Bazei de Date;

g) în soft-ul aplicat a SIAAS;

h) în sistemul operaţional;

i) în program complex antiviral;

j) în sistemul de control, gestionarea accesului şi supraveghere video;

k) în situaţii de forţă majoră (dezastre naturale);

l) alte evenimente.

m) Incidente în funcţionarea SIAAS, pot să apară la locul de muncă a unui sau mai mulţi utilizatori dintr-un sector, birou, cât şi în întregul SIAAS.

10.5.3. Recepţionarea şi înregistrarea incidentului.

a) înregistrarea şi prelucrarea incidentelor se efectuează de către colaboratorii secţiei tehnologii informaţionale şi monitorizare conform Registrului a incidentelor în domeniul securităţii informaţionale.

b) Utilizatorul se adresează secţiei tehnologii informaţionale şi monitorizare la numărul de telefon 022-820 679, iar în cazul când nu necesită intervenţie imediată, pe adresa de e-mail indicată, cu înştiinţarea despre incident;

c) Colaboratorul secţiei tehnologii informaţionale şi monitorizare primeşte cererea despre incident, în timp de 1 (un) minut înregistrează incidentul în Registrul a incidentelor în domeniul securităţii informaţionale.

d) Se înregistrează toate incidentele primite în cadrul serviciului tehnologii informaţionale şi monitorizare.

e) Colaboratorul serviciului tehnologii informaţionale şi monitorizare individual şi fără reţineri este obligat să soluţioneze incidentele, ce sunt în competenţă lui.

f) Incidentele, ce nu sunt în competenţă colaboratorului de serviciu se transmite spre soluţionare specialiştilor IT a Consiliului.

g) Specialiştii Consiliului, după primirea cererii de la persoana de serviciu în decurs de 1 (un) minut, trebuie să înceapă procedurile de eliminare a problemei înregistrate. După eliminarea incidentului, specialistul imediat raportează şefului secţiei despre finisarea lucrărilor şi a motivelor reale de apariţie a incidentului.

h) în cazul când incidentul nu poate fi înlăturat cu ajutorul colaboratorilor Consiliului, incidentul se aduce la cunoştinţa serviciilor parteneriale (CTS, BASS SYSTEM) sau altor organizaţii cu care sunt încheiate contracte corespunzătoare.

i) în cazul stabilirii incidentului ca un potenţial pericol pentru SIAAS, persoana responsabilă neîntîrziat raportează despre prezentul incident şefului secţiei tehnologii informaţionale şi monitorizare a Consiliului.

j) în cazul cînd incidentul nu poate fi înlăturat în decurs de 15 minute, şeful secţiei tehnologii informaţionale şi monitorizare asigură şi organizează şedinţa specialiştilor IT, în cadrul căruia se i-au decizii privind acţiunile ulterioare.

k) colaboratorul secţiei permanent monitorizează situaţia privind toate înregistrările incidentelor şi le ţine sub control. În cazul reţinerii nejustificate a soluţionării incidentului, raportează conducătorului, care la rîndul său i-a decizii corespunzătoare pentru soluţionarea situaţiei.

CAPITOLUL VI.
11. CONTROLUL ACCESULUI

11.1 Accesul la informaţii, la mijloacele de prelucrare a informaţiilor, precum şi la procesele de afaceri trebuie să fie gestionate în baza cerinţelor afacerii şi cerinţelor de securitate informaţională.

11.2 Controlul accesului se face conform politicii de distribuire a informaţiei şi accesului la informaţie.

11.2 Procedurile de acordare a accesului la sistemele informaţionale şi servicii vor cuprinde toată durata de existenţă a accesului, începînd de la înregistrarea noilor utilizatori pînă la anularea înregistrării utilizatorilor.

11.3 Utilizatorii vor fi atenţionaţi cu privire la obligaţia de a respecta normele de utilizare a parolelor, protecţia echipamentelor de lucru, minimizarea riscului de acces neautorizat.

11.4 Accesul la reţelele interne şi externe va fi dirijat prin:

a) autentificarea utilizatorilor şi echipamentelor;

11.5 Mijloacele de restricţionare a accesului utilizatorilor la sistemele operaţionale vor efectua:

a) autentificarea utilizatorilor;

b) înregistrarea încercărilor de autentificare reuşite şi nereuşite;

c) înregistrarea utilizării drepturilor privilegiate de sistem;

d) emiterea semnalelor de alertă în cazurile de încălcare a normelor de securitate informaţională;

e) limitarea duratei de conectare a utilizatorilor.

12 CERINŢELE AFACERII PENTRU CONTROLUL ACCESULUI
Controlul accesului la informaţie.

12.1 Politica de control al accesului

12.1.1 în scopul preîntâmpinării accesului nesancţionat la activele informaţionale ale SIAAS sunt realizate anumite acţiuni de administrare a accesului.

12.1.2 Numărul de utilizatori a SIAAS este divizat în 3 grupuri de utilizatori care activează:

a) în calitate de Colaboratori ai secţiilor/serviciilor subdiviziunilor.

b) în cadrul CNDDCM şi diviziunilor supuse.

12.1.3 Accesul utilizatorilor care activează în funcţii de Colaboratori ai direcţiilor/secţiilor subdiviziunilor este reglementat în baza ordinului Consiliului şi obligaţiunilor şi drepturilor utilizatorului din Declaraţie-Angajament.

13 ACCESULUI UTILIZATORULUI

13.1 Înregistrarea utilizătorului. Compartimentul dat descrie procedura de înregistrare a utilizatorilor şi de anulare a înregistrării pentru a garanta şi pentru a revoca accesul la SIAAS.

13.1.1 Pentru segregarea sarcinilor la înregistrarea şi acordarea drepturilor de acces a utilizatorilor SIAAS se va implementa următoarea procedură:

a) Cererea de a obţine acces la SIAAS a utilizatorilor cu conturile şi rolurile de acces care corespund funcţiei ocupată semnată de şeful diviziunii respective.

b) Admiterea accesului la SIAAS. Cererea este contrasemnată de directorul Consiliului, în cazul dacă utilizatorul activează în cadrul Consiliului.

c) întărirea accesului la SIAAS. Cererea este vizată de conducerea Consiliului.

d) Administrarea accesului la SIAAS de către colaboratorii cu drepturile respective.

13.1.2 În cazul în care utilizatorul SIAAS:

a) a fost eliberat din funcţie;

b) a fost promovat în altă funcţie;

c) se află în concediu anual;

d) se află în concediu de maternitate;

e) se află în concediu medical;

f) se află în deplasare;

13.1.3 Drepturile de acces sunt imediat anulate sau suspendate. Cererea de anulare sau suspendare a drepturilor de acces este semnată de şeful conducerea Consiliului în care activează utilizatorul respectiv, coordonată cu serviciul resursele umane, informare şi comunicare.

13.1.4 în cazul în care utilizatorul SIAAS a fost detaşat în altă diviziune a Consiliului, drepturile de acces vor fi suspendate. Cererea de suspendare a drepturilor de acces este semnată de conducerea Consiliului în care a activat utilizatorul respectiv, coordonată cu serviciul resursele umane, informare şi comunicare. Drepturile noi de acces vor fi atribuite conform procedurii de înregistrare a utilizatorului SIAAS.

13.1.5 Serviciul resursele umane, informare şi comunicare va prezenta imediat, persoanelor care administrează accesul la SIAAS, lista utilizatorilor suspendaţi din funcţie sau eliberaţi.

13.1.6 Foia de parcurs a persoanei care se eliberează se semnează numai după anularea tuturor conturilor de acces la SIAAS.

13.2 Managementul privilegiilor

13.2.1 Alocarea şi utilizarea privilegiilor trebuie restricţionată şi controlată.

13.2.2 Acordarea rolurilor privilegiate se fac numai în baza cererii vizate de conducerea Consiliului.

13.2.3 Cu o periodicitate de cel puţin odată în trei luni va fi revizuita lista utilizatorilor cu acces privilegiat.

13.3 Managementul parolei de utilizator

13.3.1 Alocarea parolelor trebuie controlată printr-un proces formal de management.

13.3.2 Staţiile de lucru, servere, software-ul instalat pe ele, şi software adiacent trebuie să fie configurat în astfel încât:

a) sa nu afişeze simbolurile parolei la tastare în mod deschis;

b) stocarea informaţiei despre parole în formă criptată sau alt tip de protecţie prin mijloacele sistemului operaţional sau aplicaţiilor software;

c) parola este necesar să conţină minimum 8 (opt) caractere alfanumerice.

13.3.3 Pentru staţiile de lucru, servere şi aplicaţiile ale sistemului informaţional pot fi utilizate măsuri suplimentare privind protecţia cu parolă:

a) la prima intrare a utilizatorului în sistem cu parolă temporară care a fost alocată de către administrator, utilizatorul să fie nevoit sa-şi introducă parola specificată de el;

b) în mod obligatoriu să se solicite de la utilizator schimbarea parolei după trei luni.

13.4 Revizuirea drepturilor de acces ale utilizatorului

13.4.1 Serviciul tehnologii informaţionale şi comunicare trebuie să revizuiască drepturile de acces ale utilizatorilor la intervale regulate utilizând un proces formal pentru aceasta.

a) Este necesar de efectua regulat analiza drepturilor de acces a utilizatorilor SIAAS utilizând proceduri oficiale.

b) Analiza drepturilor de acces a utilizatorului SIAAS se va efectua regulat o dată în 3 luni şi după fiecare modificare care a survenit în activitatea utilizatorului.

c) Analiza acordării drepturilor de acces a rolurilor privilegiate se va efectua regulat o dată în 3 luni.

d) În scopul analizei drepturilor de acces a utilizatorilor SIAAS se va utiliza schema de încadrare a Consiliului.

e) Verificarea periodica a Listei utilizatorilor SIAAS pentru a identifica drepturile de acces ce nu corespund celor specificate în cererile de acordare a drepturilor.

14 RESPONSABILITĂŢILE UTILIZATORULUI

14.1 Utilizatorul este obligat:

a) să respecte strict regulile asigurării securităţii informaţionale în lucrul cu aplicaţiile şi echipamentul SIAAS;

b) să efectueze accesul la resursele sistemului informaţional în conformitate cu drepturile de acces primite, care sunt introduse în sistemul numai pe baza cererilor scrise.

c) să păstreze în secret parola personală, cu periodicitatea stabilă să schimbe parola;

d) în lucrul cu informaţiile confidenţiale în aplicaţiile SIAAS să utilizeze mijloacele de criptare şi semnătura digitală, dacă există astfel de mijloace în aplicaţiile sistemului informaţional.

e) să execute cerinţele privind organizare a protecţiei antivirus.

f) să informeze imediat persoana responsabilă în cazul pierderii rechizitelor limitării accesului sau de suspectarea compromiterii parolelor la fel şi la depistarea:

- modificărilor neautorizate (făcute cu încălcarea modului stabilit) în configuraţie a staţiilor de lucru;

- funcţionarea incorectă a mijloacelor tehnice de protecţie instalate pe staţiile de lucru;

- procese tehnologice neprevăzute, executate de către staţia de lucru, conexiunile de cabluri şi echipamentelor periferice;

- la depistarea viruşilor sau apariţiei suspiciunii existenţei virusului;

g) imediat să acorde acces administratorilor în cazul depistării încălcării sistemului de protecţie sau suspiciunii unei asemenea încălcări.

14.2 Utilizatorului este strict interzis:

a) să folosească componentele staţiei de lucru sau activele SIAAS în scopuri personale;

b) să introducă careva schimbări de sine stătător în configuraţia ale staţiilor de lucru sau să instaleze software adăugător neprevăzute de către procesele tehnologice efectuate la staţiile de lucru;

c) să efectueze prelucrarea informaţiei confidenţiale în prezenţa persoanelor terţe (ce n-au acces la acest tip de informaţie);

d) să înscrie sau să păstreze informaţie confidenţială (ce conţine date de acces limitat) pe suporturi străine de informaţie

e) să transmită informaţie confidenţială pe canale deschise de legătură fără criptare (poşta electronică, ICQ);

f) să lese conectat fără supraveghere staţia de lucru neaccesând mijloacele de protecţie de la accesul nesancţionat (blocare temporară a ecranului şi tastaturii);

g) pe perioada lipsei temporare (concediu, boală) să transmită suporturile sale, parolele altor persoane;

h) intenţionat să folosească proprietăţile nedocumentate şi erorile din aplicaţii sau în configuraţiile mijloacelor de protecţie, care ar putea aduce la apariţia situaţiilor critice. Despre depistarea unor astfel de erori utilizatorul este obligat să aducă la cunoştinţă conducătorul Conducerii şi persoanei responsabile imediat după depistarea;

i) să deterioreze sigiliul blocurilor de sistem, să deschidă sau să încalce integritatea blocurilor de sistem şi echipamentului de reţea;

j) să conecteze de sine stătător sau să deconecteze echipamentul de reţea, să modifice configuraţia staţiei de lucru sau aparatelor de reţea, să instaleze software sau hardware. Toate schimbările trebuie să fie efectuate de către specialiştii secţiei tehnologii informaţionale şi comunicare.

k) să lanseze programe necunoscute, mai ales cele primite din surse necunoscute;

l) să încalce cerinţele securităţii informaţionale: să transmită informaţia confidenţială persoanelor străine sau organizaţiilor (baze de date, documente pentru utilizare interioară ş.a.); să deschidă schema reţelei corporative şi organizarea activităţii ei, să utilizeze oricare programe pentru aflarea parolelor, scanarea reţelei, acces nesancţionat la staţiile de lucru, hardware ş.a.

14.3 Utilizarea parolei

14.3.1 Utilizatorilor trebuie să li se ceară să urmeze bunele practici de securitate în ceea ce priveşte selecţia şi utilizarea parolelor.

14.3.2 Parolele individuale pentru intrarea iniţială în SIAAS trebuie să fie generate şi distribuite către utilizatori, centralizat, de către administratorii, cu schimbări ulterioare de sinestătător de către utilizator a parolei primite la prima înregistrare în sistemul informaţional, în caz contrar parolele rezistente la decriptare se generează imediat de către administratorul sistemului informaţional şi se face schimbarea lor peste trei luni.

14.3.3 Parolele acordate utilizatorului, trebuie să fie aduse la cunoştinţa de către persoana responsabilă. În cazul de imposibilitatea efectuării acestei acţiuni, parolele trebuie să fie transmise utilizatorilor într-un mod protejat (criptat).

14.3.4 Cerinţe către lungimea şi complexitatea parolelor:

a) parola trebuie să prezinte o secvenţă aleatoare de caractere alfa-numerice din registrele de sus sau de jos sau o combinaţie de caractere speciale (@, #, $, &, *,%, etc.), cu lungimea nu mai puţin de opt (8) simboluri;

b) parola nu trebuie să conţină informaţie de identificare uşoară, o secvenţă repetată de aceleaşi personaje, nume, date de naştere, numere de telefon, denumiri de servicii, departamente, parole simple, precum „111111", „123456", „QWERTY", etc., precum şi abrevierile generale acceptate (IBM, USER, ADMIN, etc.);

c) se interzice transmiterea parolelor către terţe părţi sau prin canale de comunicare deschisă (telefon, sms);

d) strict se interzice scrierea parolelor pe hârtie, într-un fişier, agendă electronică, precum şi alte suport de informaţie.

14.4 Echipamentul nesupravegheat de către utilizatori

14.4.1 Administratorii sistemului asigură configurarea staţiilor de lucru al utilizatorilor după cum urmează:

a) Să se efectueze blocarea calculatorului după o perioada de staţionare mai mare de 15 minute;

b) Deblocarea calculatorului să poată fi efectuată numai după introducerea parolei;

c) Să fie deconectate mijlocele de stocare;

14.5 Politica biroului curat şi a ecranului protejat

a) La plecare din birou pe masa de lucru nu trebuie să rămînă informaţii confidenţiale sau informaţii numai pentru uz de serviciu, de exemplu, pe suport de hîrtie sau pe alte suporturi electronice. Toate informaţiile trebuie încuiate în safeu sau în masa de birou;

b) Staţiile de lucru trebuie să fie deconectate sau blocate sub parolă;

c) Birourile în care se păstrează poşta de intrare/ieşire trebuie încuiate şi protejate de intrări nesancţionate;

d) Se interzice utilizarea neautorizată a echipamentelor de scanat, fotografiat sau filmat în birourile în care se conţin componente SIAAS;

e) Documentele confidenţiale trebuie extrase din echipamentele de scanare şi imprimare imediat după finisarea scanării sau imprimării lor.

15 CONTROLUL ACCESULUI LA SISTEMUL DE OPERARE

15.1 Proceduri de autentificare sigură

15.1.1 Configurarea sistemului de operare trebuie să fie făcută în aşa mod ca să corespundă cerinţelor:

a) Să nu vizualizeze identificatorii sistemului pînă cînd sistemul nu se va încărca complet;

b) Să scoată mesaj de avertizare în cazuri de conectări ne sancţionate;

c) Să limiteze numărul de încercări de conectare la sistem pînă la trei ori:

- Să fixeze încercările nereuşite;
- Să nu permită conectarea de mai departe pînă cînd nu va fi primită autorizarea administratorului;
- Să verifice lungimea minimala a parolei;

d) Să nu vizualizeze parolele introduse în sistem;

15.2 Identificarea şi autentificarea utilizatorului

Toţi utilizatorii înregistraţi în sistemul de operare trebuie sa aibă un număr de identificare unic, pentru a oferi posibilitate de analiză a operaţiunilor efectuate de utilizator în sistemul operaţional.

15.3 Sistemul de management al parolelor

15.3.1 Configurarea sistemului de operare trebuie să fie făcută în aşa mod ca să satisfacă cerinţelor:

a) Să asigure pornirea sistemului de operare numai prin introducerea parolei personale;

b) Să ofere utilizatorului modificarea parolei personale cu posibilitatea de confirmare, pentru excluderea erorilor de introducere;

c) Să nu permită introducerea parolelor simple sau scurte;

d) Să oblige modificarea parolei nu mai rar de odată în trei luni;

e) Să oblige modificarea parolelor temporare după prima conectare la sistemul operaţional;

f) Să nu permitită repetarea parolelor (utilizate anterior);

g) Să nu vizualizeze parolele la ecran;

15.4 Utilizarea programelor utilitare de sistem

15.4.1 Programe utilitare de sistem au dreptul să utilizeze numai administratorii sistemului operaţional.

15.4.2 Pauza de sistem:

a) Sesiunile inactive trebuie închise după o perioadă definită de inactivitate.

b) Mijloacele de blocare a sesiunii inactive trebuie să prevadă:

- închiderea ecranului sesiunii;
- închiderea aplicaţiilor deschise, precum şi sesiunii de reţea după o perioda mai îndelungată de inactivitate.

c) Valoarea limitei de timp ar trebui să reflecte:

- riscurile de securitate a zonei de activitate;
- clasificarea informaţiilor cu care se lucrează;
- utilizarea aplicaţiilor;
- riscurile legate de utilizatorii de echipamente.

15.5 Limitarea timpului de conectare

15.5.1 Pentru a furniza o securitate sporită a aplicaţiilor cu grad ridicat de risc trebuie utilizate restricţii cu privire la limitarea timpului de conectare.

15.5.2 Pentru aplicaţiile importante trebuie să fie prevăzute mijloace de gestiune a timpului de conexiune, în special atunci cînd se crează conexiuni din zone cu risc de securitate sporit.

15.5.3 Aceste mijloace trebuie să prevadă:

a) Un interval de timp predefinit pentru transmiterea de fişiere batch (directive/de instrucţiune) sau un timp predefinit pentru sesiunile interactive;

b) restricţia de conectare dictată de orele de lucru, daca nu sunt cerinţe de a lucra ore suplimentare;

c) re-autentificare numai după expirarea unui anumit interval de timp.

CAPITOLUL VII.
16. MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMAŢIEI

Trebuie să existe proceduri oficiale de raportare cu privire la evenimente şi proceduri oficiale de escaladare.

Toţi angajaţii trebuie să fie informaţi despre procedurile de raportare, despre diferitele tipuri de evenimente şi deficienţe care ar putea avea un impact asupra securităţii resurselor organizaţionale.

17. RAPORTAREA EVENIMENTELOR PRODUSE ŞI A SLĂBICIUNILOR PRIVIND SECURITATEA INFORMAŢIEI

17.1 Raportarea evenimentelor de securitate a informaţiei.

17.2 Persoana responsabilă de înregistrare şi monitorizarea incidentelor din cadrul SIAAS este desemnată de conducerea Consiliului şi poate fi contactată la telefonul 022-820 679.

17.3 Incidentelor securităţii informaţionale li se atribuie următoarele evenimente:

a) pierderea serviciilor prestate, lipsa funcţionării continuă a echipamentelor şi mijloacelor de prelucrare şi transmitere a informaţiilor;

b) erori de sistem sau a supraîncărcării resurselor de prelucrare şi transmitere a informaţiei;

c) erori a utilizatorilor şi a personalului TI;

d) întreruperi în SIAAS, cauzate de nerespectarea recomandărilor actelor normative şi normelor securităţii informaţionale;

e) întreruperi şi nefuncţionarea resurselor de prelucrare şi transmitere a informaţiei;

f) modificări necontrolate în sistemele de prelucrare şi transmitere a informaţiei;

g) încălcarea regulilor de acces în perimetru de securitate a Consiliului;

h) atacurile viruşilor, atacuri cibernetice şi infracţiuni, acces extern nesancţionat sau transmiterea datelor în/din SIAAS;

i) încălcarea integrităţii, accesibilităţii, confidenţialităţii, responsabilităţii, autenticităţii informaţiilor.

17.4 Incidentelor li se atribuie evenimentele, care pot apărea:

a) în sistemul de alimentare cu energie electrică în centru de prelucrare a datelor;

b) în sistemul de alimentare cu energie electrică a subdiviziunilor Consiliului;

c) în sistemul de control climateric;

d) în reţele locale (LAN, WAN) şi la echipamente;

e) la computerele personale de la locul de muncă a utilizatorilor şi la alte echipamente şi tehnologii;

f) în centru de prelucrare a datelor;

g) în sistemul administrării Bazei de Date;

h) în soft-ul aplicat a SIAAS;

i) în sistemul operaţional;

j) în program complex antiviral;

k) în sistemul de control, gestionarea accesului şi supraveghere video;

l) în situaţii de forţă majoră (dezastre naturale);

Toţi utilizatorii SIAAS sunt obligaţi să informeze momentan persoana responsabilă despre toate evenimentele de securitate a informaţiei în cadrul SIAAS.

17.5 Utilizatorul SIAAS care a depistat incidentul este obligat să întocmească un raport care conţine informaţii privind producerea incidentului pe numele şefului secţiei tehnologii informaţionale şi monitorizare.

17.5.1 În timpul depistării incidentului utilizatorul este obligat să comunice persoanei responsabile date necesare pentru diagnosticare incidentului.

17.5.2 Persoana responsabilă trebuie să înregistreze prin intermediul datele despre incident în timpul recepţionării acestuia. înregistrările despre incident trebuie să conţină următoarele date:

a) numărul unic de înregistrare;

b) clasa incidentului;

c) data/timpul creării sau modificării înregistrării;

d) numele/identificatorul specialistului sau grupului de specialişti care creează sau modifică înregistrarea de evidenţă;

e) numele/subdiviziunea/numărul de telefon/locaţia utilizatorului solicitant;

f) mijlocul de feedback;

g) descrierea simptomelor;

h) categoria sau subcategoria;

i) impactul/urgenţa/prioritatea;

j) statutul incidentului (activ, în aşteptare, închis, soluţionat, în funcţiune, nou, transmis specialistului);

k) elementele de evidenţă implicate în incident;

l) grupul de susţinere/specialistul, căruia i-a fost transmis incidentul;

m) problema/eroarea cunoscută care are legătură cu incidentul;

n) data şi timpul soluţionării;

o) categoria închiderii;

p) data şi timpul închiderii.

q) elementele de evidenţă implicate în incident.

17.5.3 Persoana responsabilă informează şeful secţiei tehnologii informaţionale şi monitorizare şi conducătorul Consiliului în care s-a produs incidentul despre cazul înregistrat.

17.5.4 Toate incidentele se înregistrează în „Registrul electronic a incidentelor în domeniul securităţii informaţiei" .

17.5.5 Şeful secţiei tehnologii informaţionale şi monitorizare va informa conducerea Consiliului despre producerea incidentului cu nivelurile de impact mediu şi mare.

17.5.6 După soluţionarea incidentului persoana responsabilă informează conducătorul Consiliului în care s-a produs incidentul, persoana care a identificat incidentul despre soluţionarea cazului.

18 MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMAŢIEI ŞI ÎMBUNĂTĂŢIRI

18.1 Trebuie să existe responsabilităţi şi proceduri, în scopul de a face faţă efectiv evenimentelor şi deficienţelor în domeniul securităţii informaţiei, îndată ce acestea vor fi comunicate.

18.2 În cazul în care sunt necesare dovezi, acestea trebuie să fie colectate pentru a se asigura îndeplinirea cerinţelor legale.

18.3 Responsabilităţi şi proceduri

18.3.1 În toate cazurile de identificarea a incidentelor în SIAAS utilizatorii sunt obligaţi să se adresează serviciului de susţinere a utilizatorilor (Hot-Line).

18.3.2 Persoana de serviciu primeşte cererea despre incident, şi înregistrează imediat şi fără reţineri incidentul în „Registrul electronic a incidentelor în domeniul securităţii informaţionale.

18.3.3 În cazul stabilirii incidentului ca un potenţial pericol pentru SIAAS, persoana responsabilă neîntârziat raportează despre prezentul incident.

18.3.4 Persoana responsabilă de sine stătător şi fără reţineri va întreprinde toate măsurile pentru soluţionarea incidentului înregistrat.

18.3.5 Incidentele, care nu pot fi soluţionate de persoana responsabilă, se transmit specialiştilor în competenţa cărora intră soluţionarea incidentului raportat cu fixarea în „Registrul electronic a incidentelor în domeniul securităţii informaţionale" a persoanei responsabile pentru soluţionarea incidentului.

18.3.6 Persoana responsabilă, după primirea cererii trebuie să înceapă procedurile de eliminare a problemei înregistrate imediat şi fără reţinere. După eliminarea incidentului, informează conducerea Consiliului despre finisarea lucrărilor şi a motivelor reale de apariţie a incidentului.

18.3.7 Persoana responsabilă fixează în „Registrul electronic a incidentelor în domeniul securităţii informaţionale" date privind soluţionarea incidentului.

18.3.8 În cazul când incidentul nu poate fi înlăturat de responsabili, incidentul se aduce la cunoştinţa serviciilor parteneriale (MOLDTELECOM, CTS,) sau altor organizaţii cu care sunt încheiate contracte corespunzătoare.

18.3.9 Specialiştii responsabili monitorizează soluţionarea incidentului şi informează conducerea Consiliului despre finisarea lucrărilor şi a motivelor reale de apariţie a incidentului.

18.3.10 Persoana responsabilă permanent monitorizează situaţia privind toate înregistrările incidentelor şi le ţine sub control. În cazul reţinerii nejustificate a soluţionării incidentului, raportează conducerii Consiliului care la rândul său i-a decizii corespunzătoare pentru soluţionarea situaţiei.

18.4 Învăţarea din incidentele de securitate a informaţiei

Nu mai rar de o dată pe lună va fi efectuată de analiză a cazurilor înregistrate în „Registrul electronic a incidentelor în domeniul securităţii informaţionale".La analiza cazurilor din „Registrul electronic a incidentelor în domeniul securităţii informaţionale" vor participa persoanele responsabile implicate.

18.4.1 În rezultatul analizelor efectuate va fi întocmit un protocol în care va fi menţionate lista acţiunilor necesare de întreprins pentru neadmiterea pe viitor a incidentelor, lista persoanelor responsabile pentru implementarea şi monitorizarea executării protocolului în cauză.

18.4.2 Vor fi stabilite metodele de soluţionare sau ocolire incidentelor analizate pentru cazurile în care incidentul se va repeta.

18.4.3 Procedura de reacţionare la incidentul analizat se va păstra la persoana responsabilă din cadrul secţiei tehnologii informaţionale şi monitorizare.

18.5 Colectarea probelor

18.5.1 Toate acţiunile descrise în capitolul curent vor fi documentate şi protocolate.

18.5.2 Toate copiile de protocoale, cereri, note informative vor fi păstrate de persoana responsabilă pentru securitatea informaţiei.

VIII. Dispoziții finale

În cazul în care legislaţia în baza căreia a fost elaborat prezentul Regulament, va fi modificată, se vor opera modificările necesare şi în conţinutul Regulamentului, în scopul aducerii acestuia în conformitate cu legislaţia în vigoare. Litigiile se vor soluţiona în conformitate cu legislaţia în vigoare a Republicii Moldova.