Anexa nr. 2
la ordinul CNTS
nr. 35-0 din 04.10.16

REGULAMENT
cu privire la asigurarea securităţii datelor cu caracter personal în sistemul informaţional automatizat Serviciului de Sînge „CTS Manager" în cadrul Centrului Naţional de Trasnfuzie a Sîngelui

I. Dispoziţii generale

1. Regulamentul la asigurarea securităţii datelor cu caracter personal în sistemul informaţional automatizat Serviciului Sînge „CTS Manager" (în continuare Regulament) în cadrul Centrului Naţional de Trasnfuzie a Sîngelui (în continuare CNTS) stabileşte responsabilităţile persoanelor din subdiviziunile structurale ale Centrului Naţional de Transfuzie a Sîngelui ce au acces la securitatea datelor cu caracter personal în cadrul Sistemului Informaţional Automatizat Serviciului Sînge "CTS Manager" (în continuare SIA Serviciul Sînge „CTS Manager").

2. Persoanele din subdiviziunile structurale ale CNTS ce au acces la securitatea datelor cu caracter personal în cadrul SIA Serviciul Sînge „CTS Manager" nu vor depăşi limitele stabilite de Politica de securitate a CNTS, precum şi normele legale stabilite prin prevederile Legilor nr.17-XVI din 15 februarie 2007 cu privire la protecţia datelor cu caracter personal şi nr. 71-XVI din 22 martie 2007 cu privire la registre, Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European TreatySeries, nr. 108, ratificate de Republica Moldova prin Hotărîrea Parlamentului nr. 483-XIV din 2 iulie 1999.

3. Regulile obligatorii ce se vor aplica în toate subdiviziunile structurale din CNTS care au acces la bunurile informaţionale a SIA Serviciul de Sînge "CTS Manager" se vor realiza prin asigurarea:

a) controlului strict asupra accesului la informaţie;
b) accesului autorizat al utilizatorului şi prevenirea accesului neautorizat la sistemele de informaţii;
c) prevenirii compromiterii sau furtului de informaţii şi a sistemelor de procesare a informaţiilor;
d) prevenirii accesului neautorizat la serviciile de reţea;
e) prevenirii accesului neautorizat la sistemele de operare;
f) prevenirii accesului neautorizat la informaţia deţinută în sistemele de aplicaţii;
g) protecţiei serviciilor interconectate;
h) securităţii informaţiei atunci când se folosesc sisteme pentru prelucrarea datelor folosind echipamente mobile şi de lucru la distanţă.

II. Organizarea măsurilor de protecţie a datelor cu caracter personal

4. Directorul CNTS desemnează persoana responsabilă de politica de securitate din cadrul CNTS şi Secţiei Tehnologii Informaţionale (în continuare STI) ca responsabili de organizarea şi asigurarea:

procedurii de înregistrare a utilizatorului şi de anulare a înregistrării pentru a garanta şi pentru a revoca accesul de monitorizare a respectării prevederilor politicii datelor cu caracter personal;

managementului de acces a utilizatorilor la activele informaţionale ale instituţiei şi monitorizează procesul de înregistrare a utilizatorilor care impune custozilor să aprobe cererea de acces.

revizuirea actelor normative în instituţie nominalizînd prin ordin persoanele care vor accesa, prelucra şi întroduce datele de caracter personal în SIA Serviciul Sînge "CTS Manager" şi responsabilitatea acestora în activitatea desfăşurată;

aprobarea listelor persoanelor cu acces la baza de date cu caracter personal;

securitatea accesului fizic în birourile unde sunt amplasate sistemele informaţionale cu conţinut de date cu caracter personal, fiind permis doar persoanele care au autorizarea necesară (conform HG nr.1123 din 14.12.2010 "Cu privire la aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal");

întegritatea şi transmiterea securizată a datelor cu caracter personal transmise;

utilizarea unei parole de acces la computerul şi sistemul lui de operare unde este instalat sistem informaţional cu conţinut de date cu caracter personal;

utilizarea unei parole de acces la sistemul de date cu caracter personal;

prelucrarea datelor cu caracter personal va fi efectuat cu consimţământul necondiţionat al subiectului datelor cu caracter personal SIA Serviciu de Sînge "CTS Manager";

politicii de securitate a datelor cu caracter personal şi revizuirea anuală ca rezultat al modificărilor sau reevaluării componentelor acesteia;

securitatea încăperii de păstrare a informaţiilor ce conţin date cu caracter personal cu alarmă, gratii, lacăt, ect.

5. Cererea de acces este aprobată de STI utilizatorului (conducătorul instituţiei) ce o lansează şi asigură că ea este în acord cu sarcinile de serviciu după cum urmează:

a) existenţa evidenţei drepturilor de acces aprobate în instituţie;
b) pregătirea personalului vizavi de faptul că acestea au înţeles condiţiile de acces;
c) drepturile de acces sunt consistente cu utilizarea documentelor;
d) accesul este audiabil şi identificabil la nivel de proces;
e) fiecare utilizator are asociat un identificator unic;
f) accesul în baza permisiunilor predefinite este restricţionat.

6. Serviciul Resurse Umane (în continuare SRU) de comun cu STI este responsabilă de atribuirea responsabilităţilor pentru implementarea procesului privind eliminarea privilegiilor de acces ale angajaţilor care îşi încheie contractele de muncă; modificarea permisiunilor accesului utilizatorilor ale căror sarcini de serviciu se modifică (în cazul avansării sau regresării în funcţie); privilegiierea de acces pentru angajaţii cu acces, care lipsesc mai mult de 5 zile din instituţie, fiind blocate pînă la clarificarea situaţiei.

6. Managementul asigurării securităţii datelor cu caracter personal în SIA Serviciul Sînge "CTS Manager" va prevedea obligatoriu:

alocarea parolelor individuale care se vor monitoriza printr-un proces cu aplicarea următoarele reguli pentru utilizatori: li se va cere să semneze o declaraţie

prin care să păstreze confidenţialitatea parolelor personale şi a parolelor de grup numai între membrii grupului (acest lucru va fi inclus în termenii şi condiţiile de angajare); în cazul cînd utilizatorii trebuie să menţină o parolă personală, li se va permite o parolă temporară iniţială, pe care utilizatorii vor fi obligaţi să o schimbe imediat după acces. Parolele temporare date în cazurile în care utilizatorii vor da uitării parolele, se vor furniza doar după identificarea utilizatorului; parolele temporare către utilizatori li se va acorda numai intr-un mod securizat;

revizuirea drepturilor de acces ale utilizatorilor la intervale regulate utilizând un proces formal pentru aceasta. Proprietarii şi custozii implementează procese formale pentru revizuirea cu regularitate a drepturilor de acces dar care obligatoriu se vor realiza: anual; trimestrial, în cazul utilizatorilor privilegiaţi; la modificarea statutului unui utilizator; la reorganizarea activităţii sau introducerii unor tehnologii noi; la modificarea politicii de acces.

7. Utilizatorilor li se va furniza accesul doar pentru serviciile pentru care au fost autorizaţi în mod specific să le utilizeze:

persoanele responsabile activează doar serviciile de reţea necesare desfăşurării activităţilor operaţionale ale instituţiei. Toate celelalte servicii de reţea sunt oprite. Accesul la resursele reţelei este permis doar utilizatorilor autorizaţi în baza principiului "celui mai mic privilegiu".

realizarea monitorizărilor manageriale a activităţii persoanelor responsabile se va efectua prin documentarea proceselor pentru managementul accesului în reţea şi obligator vor include: documentarea şi revizia monitoringului accesului autorizat; identificarea ameninţărilor şi riscurilor asociate reţelei; testarea monitorizării; asistarea proprietarilor în verificarea aplicării principiului "celui mai mic privilegiu".

8. Autentificarea utilizatorilor pentru conectarea din exterior se va asigura prin metode de autentificare corespunzătoare. Acordarea permisiunii de accesare a sistemului de la distanţă se va efectua prin: autorizarea după evaluarea riscurilor pentru fiecare serviciu în parte; conectarea securizată (de exemplu prin VPN); identificarea şi autentificarea utilizatorilor după autorizarea prealabilă a acestora.

9. Identificarea echipamentelor în reţea, autentificarea conexiunilor şi echipamentelor din locaţii specifice se va realiza prin: protecţia porturilor pentru diagnoză; asigurarea de către persoanele responsabile a controlului accesului la nivel de porturi, servicii şi sisteme pentru diagnoză, întreţinere sau monitorizare; controalele fizice şi logice vor include: mecanismele de protecţie fizică, liste de control al accesului, filtre de reţea şi sisteme de autentificare a utilizatorilor; accesul de la distanţă la porturile de diagnoză sau întreţinere se va specifica în mod explicit în acordurile/contractele cu terţii; utilizarea porturilor şi facilităţilor de diagnoză şi întreţinere este înregistrată.

10. Protecţia porturilor de diagnoză la distanţă şi a celor de configurare (accesul fizic şi logic la porturile de diagnoză şi de configurare) se vor efectua în mod sigur verificat:

controlul conexiunilor logice şi fizice se va restricţiona de persoanele responsabile, restricţionînd abilitatea utilizatorilor de a se conecta fizic şi logic la reţea. Tehnicile de restricţionare vor include: protecţia fizică a cablurilor; inspecţia fizică a punctelor de conectare din zonele publice sau sălile de şedinţă; separarea reţelelor care nu necesită dispozitive autentificate; autentificarea; reţele virtuale; scanarea contra echipamentelor neautorizate;

conectarea neautorizată în reţelele fără fire se previn prin folosirea tehnicilor de identificare şi autentificare şi se va monităriza de persoanele responsabile;

în condiţiile de separate în interiorul reţelei se va lua în considerare introducerea controlului în cadrul reţelei, pentru a separa în grupuri serviciile informatice, utilizatorii şi sistemele informatice.

11. Controlul conectării la reţea se va realiza prin capacitatea utilizatorilor de a restricţiona în conformitate cu politica de control, iar conectarea la reţea se va efectua numai prin accesul şi în corespundere cu cerinţele aplicaţiilor de afaceri. Restricţiile aplicate sunt bazate pe politica de acces şi pe cerinţele aplicaţiilor activităţilor organizaţiei şi sunt menţinute şi actualizate corespunzător. Aplicaţiile asupra cărora trebuie introduse restricţii sunt: poşta electronică; transfer unidirecţional de fişiere; transfer bidirecţional de fişiere; accesul interactiv; accesul la reţea corelat cu momentul din zi şi data accesului.

12. Controlul de rutare în reţea se va realiza prin măsuri de securitate de rutare pentru reţele pentru a se asigura că conexiunile de control al accesului pentru aplicaţiile afacerii computerului şi fluxurile de informaţii nu încalcă politica.

13. Controlul accesului la sistemul de operare se realizează prin proceduri de autentificare asigurate prin acces la sistemele de operare în mod controlat, printr-o procedură sigură de conectare. Accesul la sistemul informaţional este permis doar utilizatorilor şi proceselor autorizate:

a) şefii de subdiviziuni şi/sau persoanele responsabile se asigura că procesul de login al angajaţilor reduce oportunitatea accesului neautorizat. Aceasta va include obligatoriu: neafişarea informaţiilor despre sistem; afişarea unui mesaj de atenţionare înaintea furnizării credenţialelor de autentificare; neafişarea parolelor în clar;

b) în cazul tentativelor eşuate administratorii se vor asigura că procesul de login al custozilor este configurat astfel încât înregistrează tentativele eşuate de login; limitează numărul maxim de încercări; forţează finalizarea sesiunilor de lucru la anumite intervale orare;

c) la transmiterea parolelor proprietarii şi custozii se asigura că în timpul procesului de login parolele nu sunt transmise în clar.

14. Identificarea şi autentificarea utilizatorului se va realiza prin emiterea unui identificator unic (ID-ul utilizatorului) numai pentru uz propriu şi selectarea unei tehnici de autentificare adecvată pentru a proba identitatea pe care utilizatorul pretinde că o are.

a) la alocarea identificatorilor utilizatorilor proprietarii şi/sau persoanele responsabile se vor asigura că utilizatorii folosesc un identificator unic. Documentele şi procedurile pentru alocarea identificatorilor vor include obligator: un singur punct de contact pentru gestionarea alocării identificatorilor utilizatorilor; asigurarea că utilizatorii, cu excepţia celor privilegiaţi, nu deţin identificatori multipli; înregistrarea statutului utilizatorilor; identificarea angajaţilor sau poziţiilor care au dreptul să lanseze cereri pentru alocarea identificatorilor; confirmarea că utilizatorii au luat la cunoştinţă politicile organizaţiei; informaţii de contact cu personalul care întreţine statutul angajaţilor; revizia anuală a conformităţii statutului angajaţilor.

b) la autentificarea identificatorilor utilizatorilori proprietarii şi persoanele responsabile se vor asigura că acestea sunt autentificaţi la accesarea sistemului.

c) la partajarea identificatorilor utilizatorilor este interzisă folosirea identificatorilor partajaţi.

15. Sistemele pentru managementul parolelor vor fi interactive şi vor asigura calitatea parolelor. Se vor respecta următoarele reguli pentru stabilirea parolelor utilizatorilor: folosirea identificatorilor şi parolelor individuale; schimbarea parolelor după primul login; folosirea parolelor complexe; prevenirea reutilizării parolelor; protejarea sistemului de management al parolelor; memorarea şi transmiterea parolelor într-o formă protejată; schimbarea parolelor cu regularitate.

16. Utilizarea programelor utilitare care pot fi capabile să depăşească măsurile de securitate de sistem şi de aplicaţii vor fi restricţionate şi ferm monitorizate. Restricţionarea utilizării programelor se va realiza prin limitarea programelor: definire şi documentare a nivelurilor de autorizare; restricţionarea numărului de utilizatori cu acces la programe; revizia anuală a statutului utilizatorilor; utilizarea jurnalizată a programelor şi identificarea lor; dezinstalarea/eliminarea accesului la programele care nu servesc obiectivelor organizaţiei.

17. Sesiunile inactive trebuie închise după o perioadă definită de inactivitate. Proprietarii şi persoanele responsabile vor defini şi asigura un mecanism prin care sesiunile de lucru ale utilizatorilor sunt finalizate automat după o perioadă de inactivitate
şi se va impune reautentificarea utilizatorilor.

18. Pentru a furniza o securitate sporită a aplicaţiilor cu grad ridicat de risc se vor utiliza restricţii cu privire la limitarea timpului de conectare. Proprietarii şi persoanele responsabile vor organiza restricţionarea orelor de acces pentru aplicaţiile considerate critice. Restricţionarea operării aplicaţiilor va include limitarea accesului în cadrul unui interval de 5 minute.

19. Accesul la informaţii şi la funcţiile sistemului de aplicaţii de către utilizatori şi personalul de suport se va restricţiona în conformitate cu politica de control al accesului.

20. Utilizatorii de informaţii vor respecta bunele practici de securitate în selecţia şi utilizarea parolelor, şi anume:

la selectarea parolelor utilizatorii obligatoriu vor asigura: stabilirea parolelor complexe dar uşor de memorizat; neutilizarea aceeaşi parole pentru mai multe conturi de acces; necrearea parolelor bazate pe ceea, ce ar putea fi uşor de dedus sau obţinut din date personale, de exemplu nume, numere de telefon, date de naştere, etc., sau cu caractere identice consecutive, sau caractere exclusiv numerice sau exclusiv alfabetice.

la modificarea parolelor vor ţine cont de următoarele reguli: se va realiza la un interval specificat prin politica de securitate a parolelor; imediat după instalarea unui echipament; imediat ce un cont a fost compromis.

la prezenţa conturilor privilegiate adminstrative utilizatorii stabilesc parole de minimum 8 caractere şi le modifică pînă la maximum 40 de zile.

în protecţia şi utilizarea parolelor strict se va respecta: nedivulgarea parolei altor persoane; nedivulgarea în momentul introducerii parolei; scrierea pe orice tip de suport a parolei.

21. Utilizatorii trebuie să se asigure că echipamentul lăsat nesupravegheat este protejat în mod corespunzător şi sunt responsabili de:

securizarea locului de muncă chiar şi în situaţia în care nu sunt supervizaţi de o persoană autorizată. Securitatea locului de muncă vizează: curăţenia la locul de muncă; securitatea documentelor şi a dispozitivelor de stocare portabile; securitatea mesajelor electronice; blocarea staţiei de lucru în perioadele de inactivitate; încuierea uşilor; verificarea listingurilor imprimantelor.

comportamentul utilizatorului la locul de muncă reduce probabilitatea vizualizării neautorizate a informaţiilor, accesul sau divulgarea acestora. Comportamentul adecvat include: asigurarea că informaţiile senzitive sunt protejate contra vizualizării de către persoanele aflate în tranzit prin zona de lucru; minimizarea ecranelor calculatoarelor persoanele când sunt persoane în tranzit prin zona de lucru; protejarea documentelor de pe birouri.

22. Pentru protecţia împotriva riscurilor care decurg din folosirea echipamentelor şi comunicaţiilor mobile la distanţă sa vor asigura măsuri de securitate corespunzătoare.

23. La folosirea echipamentelor mobile (notebook-uri, palmtop-uri, laptop-uri şi telefoane mobile) sunt întreprinse măsuri pentru a preveni compromiterea informaţiei deţinute. Se vor lua în considerare riscurile lucrului cu echipamente mobile, în special în medii neprotejate. Politica de asigurare securitate acces la SIA Serviciul de Sînge "CTS Manager" şi date va include cerinţele pentru protecţia fizică, controlul accesului, tehnici criptografice, copie de siguranţă şi protecţia împotriva viruşilor, reguli şi recomandări pentru conectarea echipamentelor mobile la reţea şi îndrumări pentru utilizarea acestor echipamente în locuri publice.

24. Folosirea echipamentelor mobile conectate la reţea se va proteja în mod adecvat. Accesul de la distanţă la informaţiile de afaceri prin reţeaua publică folosind echipamente mobile va avea loc doar după ce identificarea şi autentificarea se va realiza cu succes, având instituit un mecanism potrivit de control al accesului. Echipamentele mobile sunt de asemenea protejate fizic împotriva mitului în special, de exemplu, atunci când sunt lăsate în maşini sau în alte mijloace de transport.

25. Pentru activităţile care se desfăşoară la distanţă sa va dezvolta şi implementată o politică, planuri operaţionale şi proceduri specifice acestui tip de activităţi. în cazul lucrului la distanţă se vor utiliza tehnologii de comunicaţii pentru a permite personalului lucrul la distanţă dintr-o locaţie fixă din afara organizaţiei din care fac parte. Lucrul la distanţă este autorizat şi controlat de management şi se va realiza în condiţiile adecvate pentru acest tip de lucru.

26. Se autorizează activităţile de lucru la distanţă doar dacă condiţiile adecvate de securitate şi controale sunt realizate şi acestea nu contravin politicii de securitate a acesteia.

IV. DISPOZIŢII FINALE

27. Prezentul Regulament intră în vigoare din data aprobării prin ordinul CNTS.

28. Modificarea şi completarea Regulamentului în cauză se efectuează în corespundere cu actele normative în vigoare.