

REGULAMENT
cu privire la asigurarea securității datelor cu caracter personal în sistemul
informațional automatizat Serviciului de Sânge „CTS Manager” în cadrul
Centrului Național de Transfuzie a Sângelui

I. Dispoziții generale

1. Regulamentul la asigurarea securității datelor cu caracter personal în sistemul informațional automatizat Serviciului Sânge „CTS Manager” (în continuare Regulament) în cadrul Centrului Național de Transfuzie a Sângelui (în continuare CNTS) stabilește responsabilitățile persoanelor din subdiviziunile structurale ale Centrului Național de Transfuzie a Sângelui ce au acces la securitatea datelor cu caracter personal în cadrul Sistemului Informațional Automatizat Serviciului Sânge „CTS Manager” (în continuare SIA Serviciul Sânge „CTS Manager”).
2. Persoanele din subdiviziunile structurale ale CNTS ce au acces la securitatea datelor cu caracter personal în cadrul SIA Serviciul Sânge „CTS Manager” nu vor depăși limitele stabilite de Politica de securitate a CNTS, precum și normele legale stabilite prin prevederile Legilor nr. 17-XVI din 15 februarie 2007 cu privire la protecția datelor cu caracter personal și nr. 71-XVI din 22 martie 2007 cu privire la registre, Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European Treaty Series, nr. 108, ratificate de Republica Moldova prin Hotărârea 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 informaționale a SIA Serviciul de Sânge „CTS Manager” se vor realiza prin asigurarea:
 - a) controlului strict asupra accesului la informație;
 - b) accesului autorizat al utilizatorului și prevenirea accesului neautorizat la sistemele de informații;
 - c) prevenirii compromiterii sau furtului de informații și a sistemelor de procesare a informațiilor;
 - d) prevenirii accesului neautorizat la serviciile de rețea;
 - e) prevenirii accesului neautorizat la sistemele de operare;
 - f) prevenirii accesului neautorizat la informația deținută în sistemele de aplicații;
 - g) protecției serviciilor interconectate;
 - h) securității informației atunci când se folosesc sisteme pentru prelucrarea datelor folosind echipamente mobile și de lucru la distanță.

II. Organizarea măsurilor de protecție a datelor cu caracter personal

4. Directorul CNTS desemnează persoana responsabilă de politica de securitate din cadrul CNTS și Secția Tehnologii Informaționale (în continuare STI) ca responsabili de organizarea și asigurarea:

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

managementului de acces a utilizatorilor la activele informaționale ale instituției și monitorizează procesul de înregistrare a utilizatorilor care impune custozilor să aprobe cererea de acces.

revizuirea actelor normative în instituție nominalizând prin ordin persoanele care vor accesa, prelucra și introduce datele de caracter personal în SIA Serviciul Sânge "CIS Manager" și responsabilitatea acestora în activitatea desfășurată;

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

securitatea accesului fizic în birourile unde sunt amplasate sistemele informaționale cu conținut de date cu caracter personal, fiind permis doar persoanelor care au autorizarea necesară (conform HG nr.1123 din 14.12.2010 "Cu privire la aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal");

integritatea și transmiterea securizată a datelor cu caracter personal transmise;

utilizarea unei parole de acces la computerul și sistemul lui de operare unde este instalat sistem informațional cu conținut 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 consimțământul necondiționat al subiectului datelor cu caracter personal SIA Serviciu de Sânge "CIS Manager";

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

securitatea încăperii de păstrare a informațiilor ce conțin date cu caracter personal cu alarmă, gratii, lacăt, etc.

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

- a) existența evidenței drepturilor de acces aprobate în instituție;
- b) pregătirea personalului vizavi de faptul că acestea au înțeles condițiile de acces;
- c) drepturile de acces sunt consistente cu utilizarea documentelor;
- d) accesul este audiabil și identificabil la nivel de proces;
- e) fiecare utilizator are asociat un identificator unic;
- f) accesul în baza permisiunilor predefinite este restricționat.

6. Serviciul Resurse Umane (în continuare SRU) de comun cu STI este responsabilă de atribuirea responsabilităților pentru implementarea procesului privind eliminarea privilegiilor de acces ale angajaților care își încheie contractele de muncă; modificarea permisiunilor accesului utilizatorilor ale căror sarcini de serviciu se modifică (în cazul avansării sau regresării în funcție); privilegierea de acces pentru angajații cu acces, care lipsesc mai mult de 5 zile din instituție, fiind blocate până la clarificarea situației.

6. Managementul asigurării securității datelor cu caracter personal în SIA Serviciul Sânge "CIS Manager" va prevedea obligatoriu:

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

prin care să păstreze confidențialitatea parolelor personale și a parolelor de grup numai între membrii grupului (acest lucru va fi inclus în termenii și condițiile de angajare); în cazul când utilizatorii trebuie să mențină o parolă personală, li se va permite o parolă temporară inițială, pe care utilizatorii vor fi obligați 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 într-un mod securizat;

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

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

persoanele responsabile activează doar serviciile de rețea necesare desfășurării activităților operaționale ale instituției. Toate celelalte servicii de rețea sunt oprite. Accesul la resursele rețelei este permis doar utilizatorilor autorizați în baza principiului "celui mai mic privilegiu".

realizarea monitorizărilor manageriale a activității persoanelor responsabile se va efectua prin documentarea proceselor pentru managementul accesului în rețea și obligator vor include: documentarea și revizia monitoringului accesului autorizat; identificarea amenințărilor și riscurilor asociate rețelei; 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 distanță se va efectua prin: autorizarea după evaluarea riscurilor pentru fiecare serviciu în parte; conectarea securizată (de exemplu prin VPN); identificarea și autentificarea utilizatorilor după autorizarea prealabilă a acestora.

9. Identificarea echipamentelor în rețea, autentificarea conexiunilor și echipamentelor din locații specifice se va realiza prin: protecția porturilor pentru diagnoză; asigurarea de către persoanele responsabile a controlului accesului la nivel de porturi, servicii și sisteme pentru diagnoză, întreținere sau monitorizare; controalele fizice și logice vor include: mecanismele de protecție fizică, liste de control al accesului, filtre de rețea și sisteme de autentificare a utilizatorilor; accesul de la distanță la porturile de diagnoză sau întreținere se va specifica în mod explicit în acordurile/contractele cu terții; utilizarea porturilor și facilităților de diagnoză și întreținere este înregistrată.

10. Protecția porturilor de diagnoză la distanță și a celor de configurare (accesul fizic și logic la porturile de diagnoză și de configurare) se vor efectua în mod sigur verificat:

controlul conexiunilor logice și fizice se va restricționa de persoanele responsabile, restricționând abilitatea utilizatorilor de a se conecta fizic și logic la rețea. Tehnicile de restricționare vor include: protecția fizică a cablurilor; inspecția fizică a punctelor de conectare din zonele publice sau sălile de ședință; separarea rețelelor care nu necesită dispozitive autentificate; autentificarea; rețele virtuale; scanarea contra echipamentelor neautorizate;

conectarea neautorizată în rețelele fără fire se previn prin folosirea tehnicilor de identificare și autentificare și se va monitoriza de persoanele responsabile;

în condițiile de separate în interiorul rețelei se va lua în considerare introducerea controlului în cadrul rețelei, pentru a separa în grupuri serviciile informatice, utilizatorii și sistemele informatice.

11. Controlul conectării la rețea se va realiza prin capacitatea utilizatorilor de a restricționa în conformitate cu politica de control, iar conectarea la rețea se va efectua numai prin accesul și în corespundere cu cerințele aplicațiilor de afaceri. Restricțiile aplicate sunt bazate pe politica de acces și pe cerințele aplicațiilor activităților organizației și sunt menținute și actualizate corespunzător. Aplicațiile asupra cărora trebuie introduse restricții sunt: poșta electronică; transfer unidirecțional de fișiere; transfer bidirecțional de fișiere; accesul interactiv; accesul la rețea corelat cu momentul din zi și data accesului.

12. Controlul de rutare în rețea se va realiza prin măsuri de securitate de rutare pentru rețele pentru a se asigura că conexiunile de control al accesului pentru aplicațiile afacerii computerului și fluxurile de informații 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 informațional este permis doar utilizatorilor și proceselor autorizate:

a) șefii de subdiviziuni și/sau persoanele responsabile se asigura că procesul de login al angajaților reduce oportunitatea accesului neautorizat. Aceasta va include obligatoriu: neafișarea informațiilor despre sistem; afișarea unui mesaj de atenționare înaintea furnizării credențialelor de autentificare; neafișarea parolelor în clar;

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

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

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

a) la alocarea identificatorilor utilizatorilor proprietarii și/sau persoanele responsabile se vor asigura că utilizatorii folosesc un identificator unic. Documentele și procedurile pentru alocarea identificatorilor vor include obligatoriu: un singur punct de contact pentru gestionarea alocării identificatorilor utilizatorilor; asigurarea că utilizatorii, cu excepția celor privilegiați, nu dețin identificatori multipli; înregistrarea statutului utilizatorilor; identificarea angajaților sau pozițiilor care au dreptul să lanseze cereri pentru alocarea identificatorilor; confirmarea că utilizatorii au luat la cunoștință politicile organizației; informații de contact cu personalul care întreține statutul angajaților; revizia anuală a conformității statutului angajaților.

b) la autentificarea identificatorilor utilizatorilor proprietarii și persoanele responsabile se vor asigura că acestea sunt autentificați la accesarea sistemului.

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

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

16. Utilizarea programelor utilitare care pot fi capabile să depășească măsurile de securitate de sistem și de aplicații vor fi restricționate și ferm monitorizate. Restricționarea utilizării programelor se va realiza prin limitarea programelor: definire și documentare a nivelurilor de autorizare; restricționarea numărului de utilizatori cu acces la programe; revizia anuală a statutului utilizatorilor; utilizarea jurnalizată a programelor și identificarea lor; dezinstalarea/eliminarea accesului la programele care nu servesc obiectivelor organizației.

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

și se va impune reautentificarea utilizatorilor.

18. Pentru a furniza o securitate sporită a aplicațiilor cu grad ridicat de risc se vor utiliza restricții cu privire la limitarea timpului de conectare. Proprietarii și persoanele responsabile vor organiza restricționarea orelor de acces pentru aplicațiile considerate critice. Restricționarea operării aplicațiilor va include limitarea accesului în cadrul unui interval de 5 minute.

19. Accesul la informații și la funcțiile sistemului de aplicații de către utilizatori și personalul de suport se va restricționa în conformitate cu politica de control al accesului.

20. Utilizatorii de informații vor respecta bunele practici de securitate în selecția și utilizarea parolelor, și anume:

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

la modificarea parolelor vor ține 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 prezența conturilor privilegiate administrativ, utilizatorii stabilesc parole de minimum 8 caractere și le modifică până la maximum 40 de zile.

în protecția și 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 și sunt responsabili de:

securizarea locului de muncă chiar și în situația în care nu sunt supervizați de o persoană autorizată. Securitatea locului de muncă vizează: curățenia la locul de muncă; securitatea documentelor și a dispozitivelor de stocare portabile; securitatea mesajelor electronice; blocarea stației de lucru în perioadele de inactivitate; încuierea ușilor; verificarea listingurilor imprimantelor.

comportamentul utilizatorului la locul de muncă reduce probabilitatea vizualizării neautorizate a informațiilor, accesul sau divulgarea acestora. Comportamentul adecvat include: asigurarea că informațiile sensitive 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 protecția împotriva riscurilor care decurg din folosirea echipamentelor și comunicațiilor mobile la distanță se vor asigura măsuri de securitate corespunzătoare.

23. La folosirea echipamentelor mobile (notebook-uri, palmtop-uri, laptop-uri și telefoane mobile) sunt întreprinse măsuri pentru a preveni compromiterea informației deținute. Se vor lua în considerare riscurile lucrului cu echipamente mobile, în special în medii neprotejate. Politica de asigurare securitate acces la SIA Serviciul de Sânge "CIS Manager" și date va include cerințele pentru protecția fizică, controlul accesului, tehnici criptografice, copie de siguranță și protecția împotriva virusilor, reguli și recomandări pentru conectarea echipamentelor mobile la rețea și îndrumări pentru utilizarea acestor echipamente în locuri publice.

24. Folosirea echipamentelor mobile conectate la rețea se va proteja în mod adecvat. Accesul de la distanță la informațiile de afaceri prin rețeaua publică folosind echipamente mobile va avea loc doar după ce identificarea și autentificarea se va realiza cu succes, având instituit un mecanism potrivit de control al accesului. Echipamentele mobile sunt de asemenea protejate fizic împotriva furtului în special, de exemplu, atunci când sunt lăsate în mașini sau în alte mijloace de transport.

25. Pentru activitățile care se desfășoară la distanță se va dezvolta și implementată o politică, planuri operaționale și proceduri specifice acestui tip de activități. În cazul lucrului la distanță se vor utiliza tehnologii de comunicații pentru a permite personalului lucrul la distanță dintr-o locație fixă din afara organizației din care fac parte. Lucrul la distanță este autorizat și controlat de management și se va realiza în condițiile adecvate pentru acest tip de lucru.

26. Se autorizează activitățile de lucru la distanță doar dacă condițiile adecvate de securitate și controale sunt realizate și acestea nu contravin politicii de securitate a acesteia.

IV. DISPOZIȚII FINALE

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

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