MINISTERUL SĂNĂTĂȚII AL REPUBLICII MOLDOVA
IMSP SPITALUL CLINIC DE PȘIHIATRIE

ORDIN

Nr. 47a din „17" 03 2022

Cu privire la aprobarea și implementarea Politicii interne de securitate cibernetică în cadrul IMSP Spitalul Clinic de Psihiatrie

În temeiul Hotărârii Guvernului nr. 201 din 28.03.2017 „privind aprobarea cerințelor minime obligatorii de securitate cibernetică", în scopul aplicării cerințelor minime de securitate cibernetică față de echipamente (hardware) și produse de program (software), precum și sistemele informatice, resursele și sistemele informaționale existente în cadrul IMSP Spitalul Clinic de Psihiatrie, cît și în corespundere cu Regulamentul de organizare și funcționare a instituției,

ORDON:

1. Se aprobă Politica internă de securitate cibernetică în cadrul IMSP Spitalul Clinic de Psihiatrie, anexa nr.1 pentru aplicarea cerințelor de securitate cibernetică.
2. Se desemnează Dl. Virgiliu Gîlcă, Șef Serviciul tehnologii informaționale și comunicații, în calitate de persoană responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în cadrul IMSP Spitalul Clinic de Psihiatrie.
3. Serviciul secretariat și relații publice, D-na Ioana Ivanov va aduce la cunoștință prezentul ordin persoanelor vizate, sub semnătură.
4. Controlul asupra executării prezentului Ordin mi-l asum.

Director **Victor Furtună**

Executor: Gîlcă Virgiliu
Avizat: Boaghe Vasile

Anexa nr. 1 la ordinul nr. 47-a din 18.09.2022

APROB

Director IMSP Spitalul Clinic de Psihiatrie

_____ Furtună Victor

Politica internă de securitate cibernetică în cadrul IMSP Spitalul Clinic de Psihiatrie

I. Preambul

1. Dezvoltarea accelerată a tehnologiilor informaţiei şi de comunicaţii moderne ridică la un alt nivel abordarea ameninţărilor, riscurilor şi vulnerabilităţilor într-o societate informaţională. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvenţă, o complexitate şi o amploare din ce în ce mai mare, aducând pagube enorme sectorului guvernamental, celui privat şi cetăţenilor, ca urmare a caracterului lor asimetric. Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic constituie constrângeri la nivel global. Ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală. Prejudiciile economice provenite din exploatarea unor asemenea vulnerabilităţi sunt destul de semnificative.

II. Introducere

2. Prezenta Politică este aprobată, inclusiv, în vederea conformării cu prevederile Hotărârii Guvernului Republicii Moldova nr.201 din data de 28 martie 2017 "*privind aprobarea Cerinţelor minime obligatorii de securitate cibernetică*"

3. În sensul prezentei Politici, următoarele noţiuni principale semnifică:

audit de securitate cibernetică - evaluare sistemică, detaliată, măsurabilă şi tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, cu emiterea de recomandări pentru minimizarea riscurilor identificate;

securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri pro-active şi reactive prin care în spaţiul cibernetic se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea informaţiilor în format electronic, a sistemelor şi resurselor informaţionale, a serviciilor publice şi private. Măsurile pro-active şi reactive includ politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protecţie a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor;

risc de securitate în spaţiul cibernetic - probabilitate ca o ameninţare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

vulnerabilitate - ineficacitate în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.

incident cibernetic - eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;
sistemul de management al securităţii cibernetice – toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilităţile, resursele şi structurile care sunt folosite pentru a proteja şi păstra intactă informaţia;
cerinţe minime obligatorii de securitate cibernetică –realizează prin sistemul de management al securităţii cibernetice şi se aplică faţă de:
soft-ware - se înţelege un sistem de programe pentru calculatoare incluzând procedurile lor de aplicare, sistem furnizat odată cu calculatorul respectiv sau creat ulterior de către utilizator sau şi cumpărat din comerţ;
hard-ware - este partea fizică a unui sistem informatic, constituită din ansamblul de componente electrice, electronice şi mecanice care împreună pot primi, prelucra, stoca şi reda informaţii, sub diverse forme de semnale electrice, acustice sau optice;

III, Scopul, obiectivele şi domeniul de activitate

4. Politica internă privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi asigurarea colectării, procesării, stocării şi accesării în siguranţă a datelor, inclusiv a datelor de interes public.
5. Politica internă privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie se aplică în cadrul instituţiei faţă de:
1) echipamentele (hardware) şi produsele de program (software);
2) sistemele informatice, resursele şi sistemele informaţionale (în continuare - sisteme), precum şi cele aliate la etapa de elaborare, testare şi implementare.
6. Realizarea scopului Politicii interne privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie, presupune atingerea următoarelor obiective:
1) Respectarea/punerea în aplicare a prevederilor cadrului legislativ-normativ naţional şi internaţional, inclusiv a standardelor, în domeniul securităţii cibernetice;
2) Implementarea procedurilor de securitate cibernetică în scopul respectării Cerinţelor minime obligatorii de securitate cibernetică, aprobate prin actele normative;
3) Implementarea măsurilor organizaţionale direcţionale spre reglementarea internă a procedurilor de securitate cibernetică;
4) Prevenirea accesului neautorizat la sistemele instituţiei;
5) Garantarea funcţionării neîntrerupte şi în siguranţă a sistemelor instituţiei;
6) Asigurarea intervenţiei prompte, eficiente şi sistematice la incidentele dc Securitate cibernetică;
7) Sporirea calificării angajaţilor instituţiei în domeniul securităţii cibernetice;
8) Realizarea măsurilor de evaluare şi management a riscurilor cibernetice, sporirea nivelului de protecţie a sistemelor, hardware şi software ale instituţiei.
7. Scopul securităţii cibernetice este de a proteja sistemele, echipamentele şi produsele de program ale instituţiei, de a asigura continuitatea activităţii şi de a minimiza daunele aduse instituţiei prin prevenirea şi minimizarea impactului incidentelor de securitate.

IV. Principiile de organizare internă a managementului de securitate cibernetică

8. Sistemul de management al securităţii cibernetice a IMSP Spitalul Clinic de Psihiatrie are la bază următoarele principii:

1) *confidenţialitatea* - asigurarea faptului că informaţia este accesibilă doar persoanelor autorizate. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemele informaţionale;

2) *integritatea* - păstrarea acurateţei şi completitudinii informaţiei, precum şi a metodelor de procesare;

3) *disponibilitatea* - asigurarea faptului că utilizatorii autorizaţi au acces la informaţie şi la resursele asociate atunci cînd este necesar. Diverse software necesită nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a sistemelor informaţionale;

4) *nonrepudierea* - asigurarea faptului că, după emiterea/recepţionarea unei informaţii într-un sistem, de comunicaţii securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informaţiile în cauză.

V. Analiza situaţiei şi vulnerabilităţilor

9. Pentru implementarea politicii interne privind securitatea cibernetică, se efectuează un audit intern de securitate cibernetică, care cuprinde următoarele chestiuni:

l) Evaluarea vulnerabilităţilor/riscurilor: se identifică ameninţările asupra resurselor şi ameninţările care trebuie eliminate şi/sau care pot fi tolerate, se evaluează vulnerabilitatea faţă de aceste ameninţări şi probabilitatea de producere a lor şi se estimează impactul potenţial, ierarhizarea riscurilor;

2) Identificarea sistemelor, echipamentelor şi produselor de program care trebuie protejate şi la ce nivel;

3) Mijloacele, prin care urmează a fi implementată securitatea cibernetică;

4) Resursele financiare, umane, sociale etc. necesare pentru întreprinderea măsurilor de securitate cibernetică.

VI. Declaraţia managementului IMSP Spitalul Clinic de Psihiatrie de susţinere a scopului şi principiilor politicii interne privind securitatea cibernetică a instituţiei

10. Conducerea IMSP Spitalul Clinic de Psihiatrie îşi asumă responsabilitatea pentru organizarea şi gestionarea activităţii privind menţinerea şi îmbunătăţirea sistemului de management al securităţii cibernetice.

VII. Respectarea şi implementarea politicii inlerne privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie

11. Şeful Serviciului tehnologii informaţionale şi comunicaţii, este responsabil de punerea în aplicare a sistemului de management al securităţii cibernetice în cadrul IMSP Spitalul Clinic de Psihiatrie, întreprinde toate măsurile necesare pentru protecţia sistemelor, echipamentelor şi produselor de program împotriva ameninţărilor interne sau externe, deliberate sau accidentale, pentru a asigura că:

1) informaţiile, serviciile şi sistemele sunt protejate împotriva accesului neautorizat;

2) confidenţialitatea informaţiilor este păstrată;

3) integritatea informaţiilor, serviciilor şi a sistemelor este păstrată;

4) disponibilitatea informaţiilor, serviciilor şi sistemelor este asigurată atunci cînd procesele activităţii o cer;

5) cerinţele şi obiectivele organizaţionale sunt îndeplinite;
6) cerinţele legislative şi de reglementare sunt îndeplinite.
12. Prevederile Politicii interne privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie, a Regulamentelor şi procedurilor se respectă şi se aplică nediscriminatoriu de către toţi angajaţii instituţiei cărora li s-a autorizat accesul la sistemele, echipamentele şi produsele de program, precum şi altor persoane fizice şi juridice (consultanţi, experţi, stagiari, etc.).
13. Fiecare utilizator autorizat al sistemelor, echipamentelor şi produselor de program ale IMSP Spitalul Clinic de Psihiatrie poartă răspundere personală pentru aplicarea întocmai în activitatea sa a regulamentelor şi procedurilor de securitate cibernetică în vigoare, elaborate şi aprobate, conform standardelor internaţionale, legislaţiei naţionale, legislaţiei speciale şi a reglementărilor interne de funcţionare. De asemenea, orice utilizator autorizat al sistemelor, echipamentelor şi produselor de program are obligaţia raportării oricărui incident de securitate.
14. Nerespectarea Politicii interne privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie atrage după sine aplicarea măsurilor disciplinare, precum şi revizuirea drepturilor de acces la informaţie.
15. Dacă este necesar, politica internă privind securitatea cibernetică a IMSP Spitalul Clinic de Psihiatrie este revizuită în vederea actualizării şi adaptării la noile condiţii şi cerinţe.

Întocmit: Gîlcă V./Şef STIC
Avizat: Dilan L./Ofiţer date cu caracter personal
Avizat: Boaghe V./Şef serviciul juridic şi achiziţii publice