MINISTERUL SĂNĂTĂȚII, MUNCII ȘI PROTECȚIEI SOCIALE AL REPUBLICII MOLDOVA
**AGENȚIA NAȚIONALĂ PENTRU SĂNĂTATE PUBLICĂ**

MD 2028, mun. Chișinău, str. Gh. Asachi 67A, Tel. +373 22 574 501:Fax. +373 22 729 725,
http://www.ansp.md; e-mail:office@ansp.md IDNO:1018601000021

# ORDIN

Nr. 391 din „ 01 „ august 2019

**Cu privire la aprobarea politicii interne privind securitatea cibernetică a Agenției Naționale pentru Sănătate Publică**

În temeiul pct.3 a Hotărîrii Guvernului nr.201 din 28.03.2017 cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică față de: echipamentele (hardware), produsele de program (software) existente în ANSP și sistemele informatice, resursele și sistemele informaționale existente în instituție, precum și cele aflate la etapa de elaborare, testare și implementare,

**ORDON:**

1. Se aprobă Politica internă privind Securitatea cibernetică a Agenției Naționale pentru Sănătate Publică (ANSP) conform anexei.
2. Se desemnează dl. Sergiu Stigariov, șef Direcție TIC, responsabil de punerea în aplicare a sistemului de management al securității cibernetice în ANSP.
3. Șefii de Direcții și Centrelor de Sănătate Publică teritoriale:
   3.1. vor aduce la cunoștință personalului din subordine prevederile prezentului ordin contra semnătură;
   3.2. vor alcătui listele produselor de program (software) existente și sistemelor informaționale cu persoanele care le folosesc;
   3.3. listele vor fi remise dl. Sergiu Stigariov pînă la data de 30.08.2019
4. Controlul realizării prezentului ordin mi-l asum.

**Director interimar** **Nicolae FURTUNĂ**

Anexa nr.1
la ordinul ANSP
nr. _391_ din 01 august_ 2019

# POLITICA INTERNĂ PRIVIND SECURITATEA CIBERNETICĂ A AGENȚIEI NAȚIONALE PENTRU SĂNĂTATE PUBLICĂ

CUPRINS:

## I. PREAMBUL

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 mari, 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 sânt destul de semnificative.

## II. ÎNTRODUCERE

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, Publicat: 07.04.2017 în Monitorul Oficial Nr. 109-118 art. Nr: 277 şi Hotărârii Guvernului Republicii Moldova Nr. 811 din 29.10.2015 cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, Publicat: 13.11.2015 în Monitorul Oficial Nr. 306-310 art. Nr: 905

## III. NOŢIUNI GENERALE

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

***incident cibernetic*** – eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

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

***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 şi non-repudierea 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;

***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 de-a gata.

***test de penetrare*** – evaluare a securităţii cibernetice a unui sistem împotriva diferitor tipuri de atacuri;

***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;

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

## IV. SCOPUL, OBIECTIVELE ŞI DOMENIUL DE ACTIVITATE

1. Politica internă privind securitatea cibernetică a Agenţiei Naţionale pentru Sănătate Publică 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.

2. Politica internă privind securitatea cibernetică a Agenţiei Naţionale pentru Sănătate Publică se aplică în cadrul Agenţiei Naţionale pentru Sănătate Publică faţă de:

- echipamentele (hardware) şi produsele de program (software) existente în cadrul fiecărei instituţii;
- sistemele informatice, resursele şi sistemele informaţionale existente în instituţie (în continuare - sisteme), precum şi cele aliate la etapa de elaborare, testare şi implementare.

3. Realizarea scopului Politicii interne privind securitatea cibernetică a Agenţiei Naţionale pentru Sănătate Publică, presupune atingerea următoarelor *obiective*:

- Respectarea/punerea în aplicare a prevederilor cadrului legislativ - normativ naţional şi internaţional, inclusiv a standardelor, în domeniul securităţii cibernetice;
- Implementarea procedurilor de securitate cibernetică în scopul respectării Cerinţelor minime obligatorii de securitate cibernetică, aprobate prin Hotărîrea Guvernului nr. 201 din 28.03.2017;
- Implementarea măsurilor organizaţionale direcţionate spre reglementarea internă a procedurilor de securitate cibernetică;
- Prevenirea accesului neautorizat la sistemele Agenţiei Naţionale pentru Sănătate Publică;
- Garantarea funcţionării neîntrerupte şi în siguranţă a sistemelor Agenţiei Naţionale pentru Sănătate Publică;
- Asigurarea intervenţiei prompte, eficiente şi sistematice la incidentele de securitate cibernetică;
- Sporirea calificării angajaţilor Agenţiei Naţionale pentru Sănătate Publică în domeniul securităţii cibernetice;
- Realizarea măsurilor de evaluare şi management a riscurilor de securitate în spaţiul cibernetic ale Agenţiei Naţionale pentru Sănătate Publică, sporirea nivelului de protecţie a sistemelor, hard-ware şi soft-ware ale Agenţiei Naţionale pentru Sănătate Publică.

1. Scopul securităţii cibernetice este de a proteja sistemele, echipamentele şi produsele de program ale Agenţiei Naţionale pentru Sănătate Publică, de a asigura continuitatea activităţii şi de a minimiza daunele aduse Agenţiei Naţionale pentru Sănătate Publică prin prevenirea şi minimizarea impactului incidentelor de securitate.

## V. PRINCIPIILE DE ORGANIZARE INTERNĂ A MANAGEMENTULUI DE SECURITATE CIBERNETICĂ

5. Sistemul de management al securităţii cibernetice a Agenţiei Naţionale pentru Sănătate Publică are la bază următoarele principii:

- confidenţialitatea - asigurarea faptului că informaţia este accesibilă doar persoanelor autorizate. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemele informaţionale;
- integritatea - păstrarea acurateţei şi completitudinii informaţiei, precum şi a metodelor de procesare;
- disponibilitatea - asigurarea faptului că utilizatorii autorizaţi au acces la informaţie şi la resursele asociate atunci când este necesar. Diverse

software necesită nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urm are a nefuncţionării corespunzătoare a sistemelor informaţionale:

- non-repudierea - 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.

## VI. ANALIZA SITUAŢIEI ŞI VULNERABILITĂŢILOR

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

- 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;
- Efectuarea testelor de penetrare;
- Ierarhizarea riscurilor;
- Identificarea sistemelor, echipamentelor şi produselor de program care trebuie protejate şi la ce nivel;
- Mijloacele, prin care urmează a fi implementată securitatea cibernetică;
- Resursele financiare, umane, sociale etc. necesare pentru întreprinderea
- măsurilor de securitate cibernetică.

## VII. DECLARAŢIA MANAGEMENTULUI AGENŢIEI NAŢIONALE PENTRU SĂNĂTATE PUBLICĂ DE SUSŢINERE A SCOPULUI ŞI PRINCIPIILOR POLITICII INTERNE PRIVIND SECURITATEA CIBERNETICĂ A AGENŢIEI NAŢIONALE PENTRU SĂNĂTATE PUBLICĂ

7. Conducerea Agenţiei Naţionale pentru Sănătate Publică îşi asumă responsabilitatea pentru organizarea şi gestionarea activităţii privind menţinerea şi îmbunătăţirea sistemului de management al securităţii cibernetice.

## VIII. RESPECTAREA ŞI IMPLEMENTAREA POLITICII INTERNE PRIVIND SECURITATEA CIBERNETICĂ A AGENȚIEI NAȚIONALE PENTRU SĂNĂTATE PUBLICĂ

8. Persoana (subdiviziunea), responsabilă de punerea în aplicare a sistemului de management al securităţii cibernetice în instituţie, întreprinde toate măsurile necesare pentru protecţia sistemelor, echipamentelor şi produselor de program împotriva ameninţărilor interne sau externe, deliberate sau accidentale, pentru a asigura că:

- informaţiile, serviciile şi sistemele sunt protejate împotriva accesului neautorizat;
- confidenţialitatea informaţiilor este păstrată;
- integritatea informaţiilor, serviciilor şi a sistemelor este păstrată;
- disponibilitatea informaţiilor, serviciilor şi sistemelor este asigurată atunci când procesele activităţii o cer;
- cerinţele şi obiectivele organizaţionale sunt îndeplinite;
- cerinţele legislative şi de reglementare sunt îndeplinite.

9. Prevederile Politicii interne privind securitatea cibernetică a Agenției Naționale pentru Sănătate Publică, a Regulamentelor şi procedurilor se respectă şi se aplică nediscriminatoriu de către toţi angajaţii Agenției Naționale pentru Sănătate Publică cărora li s-a autorizat accesul la sistemele, echipamente şi produse de program, precum şi altor persoane fizice şi juridice (consultanţi, experţi, stagiari, etc.).

10. Fiecare utilizator autorizat al sistemelor, echipamentelor şi produselor de program a Agenției Naționale pentru Sănătate Publică 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 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.

11. Nerespectarea Politicii interne privind securitatea cibernetică a Agenției Naționale pentru Sănătate Publică atrage după sine aplicarea unor măsuri disciplinare, precum şi revizuirea drepturilor de acces la informaţie.

12. Politica internă privind securitatea cibernetică a Agenției Naționale pentru Sănătate Publică este revizuită anual în vederea actualizării şi adaptării la noile condiţii şi cerinţe.