



Ministerul Economiei
și Infrastructurii
al Republicii Moldova

ORDIN

Nr. 402 din "28" 12 2017

mun. Chișinău

*Cu privire la aprobarea politicii interne
privind securitatea cibernetică a
Ministerului Economiei și Infrastructurii*

În temeiul prevederilor pct.3 din Hotărîrea Guvernului nr.201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art.277),

ORDON:

1. Se aprobă Politica internă privind securitatea cibernetică a Ministerului Economiei și Infrastructurii conform anexei.

2. Se desemnează dl. Veaceslav VOLCOV, Șef Serviciul tehnologiei informației și comunicațiilor, în calitate de persoană responsabilă de punerea în aplicare a sistemului de management al securității cibernetică în cadrul Ministerului Economiei și Infrastructurii.

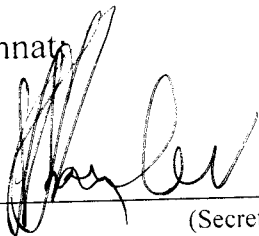
3. Angajații ministerului cărora li s-a autorizat accesul la sistemele, echipamentele și produsele de program poartă răspundere personală pentru respectarea prevederilor prezentului Ordin.

4. Controlul asupra executării prezentului Ordin mi-l asum.

Secretar General de Stat

Iulia COSTIN

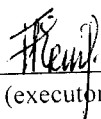
Contrasemnata



(Secretari de stat)

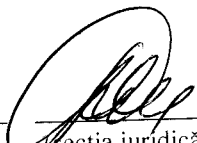
(Secretar general de stat)

Vizat:

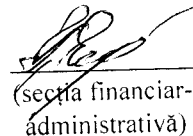


(executor)

(direcția/secția)




(secția juridică)



(secția financiar-administrativă)

Coordonat:



(subdiviziunile structurale interesate)

Politica internă privind securitatea cibernetică a Ministerului Economiei și Infrastructurii

I. Scopul, obiectivele și domeniul de activitate

1. Politica internă privind securitatea cibernetică a Ministerului Economiei și Infrastructurii are ca *scop* asigurarea integrității, confidențialității și disponibilității informației, precum și asigurarea colectării, procesării, stocării și accesării în siguranță a datelor, inclusiv a datelor de interes public.

2. Politica internă privind securitatea cibernetică a Ministerului Economiei și Infrastructurii se aplică în cadrul instituției față de:

- 1) echipamentele (hardware) și produsele de program (software);
- 2) sistemele informatice, resursele și sistemele informaționale (în continuare - sisteme), precum și cele aliate la etapa de elaborare, testare și implementare.

3. Realizarea scopului Politicii interne privind securitatea cibernetică a Ministerului Economiei și Infrastructurii, presupune atingerea următoarelor *obiective*:

- 1) Respectarea/punerea în aplicare a prevederilor cadrului legislativ-normativ național și internațional, inclusiv a standardelor, în domeniul securității cibernetică;
- 2) Implementarea procedurilor de securitate cibernetică în scopul respectării Cerințelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201 din 28 martie 2017;
- 3) Implementarea măsurilor organizaționale direcționate spre reglementarea internă a procedurilor de securitate cibernetică;
- 4) Prevenirea accesului neautorizat la sistemele instituției;
- 5) Garantarea funcționării neîntrerupte și în siguranță a sistemelor instituției;
- 6) Asigurarea intervenției prompte, eficiente și sistematice la incidentele de securitate cibernetică;
- 7) Sporirea calificării angajaților instituției în domeniul securității cibernetică;
- 8) Realizarea măsurilor de evaluare și management a riscurilor cibernetică, sporirea nivelului de protecție a sistemelor, hardware și software ale instituției.

4. Scopul securității cibernetică este de a proteja sistemele, echipamentele și produsele de program ale instituției, de a asigura continuitatea activității și de a minimiza daunele aduse instituției prin prevenirea și minimizarea impactului incidentelor de securitate.

II. Principiile de organizare internă a managementului de securitate cibernetică

5. Sistemul de management al securității cibernetică a Ministerului Economiei și Infrastructurii are la bază următoarele principii:

1) *confidențialitatea* - asigurarea faptului că informația este accesibilă doar persoanelor autorizate. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la sistemele informaționale;

2) *integritatea* - păstrarea acurateței și completitudinii informației, precum și a metodelor de procesare;

3) *disponibilitatea* - asigurarea faptului că utilizatorii autorizați au acces la informație și la resursele asociate atunci când este necesar. Diverse software necesită nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a sistemelor informaționale;

4) *nonrepudierea* - asigurarea faptului că, după emiterea/recepționarea unei informații într-un sistem de comunicații securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expedit/primit informațiile în cauză.

III. Analiza situației și vulnerabilităților

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

1) Evaluarea vulnerabilităților/riscurilor: se identifică amenințările asupra resurselor și amenințările care trebuie eliminate și/sau care pot fi tolerate, se evaluează vulnerabilitatea față de aceste amenințări și probabilitatea de producere a lor și se estimează impactul potențial, ierarhizarea riscurilor;

2) Identificarea sistemelor, echipamentelor și produselor de program care trebuie protejate și 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.

IV. Declarația managementului Ministerului Economiei și Infrastructurii de susținere a scopului și principiilor politicii interne privind securitatea cibernetică a instituției

7. Conducerea instituției își asumă responsabilitatea pentru organizarea și gestionarea activității privind menținerea și îmbunătățirea sistemului de management al securității cibernetică.

V. Respectarea și implementarea politicii interne privind securitatea cibernetică a Ministerului Economiei și Infrastructurii

8. Șeful Serviciului tehnologiei informației și comunicațiilor, responsabil de punerea în aplicare a sistemului de management al securității cibernetică în cadrul Ministerului, întreprinde toate măsurile necesare pentru protecția sistemelor, echipamentelor și produselor de program împotriva amenințărilor interne sau externe, deliberate sau accidentale, pentru a asigura că:

- 1) informațiile, serviciile și sistemele sunt protejate împotriva accesului neautorizat;
- 2) confidențialitatea informațiilor este păstrată;
- 3) integritatea informațiilor, serviciilor și a sistemelor este păstrată;
- 4) disponibilitatea informațiilor, serviciilor și sistemelor este asigurată atunci când procesele activității o cer;
- 5) cerințele și obiectivele organizaționale sunt îndeplinite;
- 6) cerințele legislative și de reglementare sunt îndeplinite.

9. Prevederile Politicii interne privind securitatea cibernetică a Ministerului Economiei și Infrastructurii, a Regulamentelor și procedurilor se respectă și se aplică nediscriminatoriu de către toți angajații Ministerului cărora li s-a autorizat accesul la sistemele, echipamentele și produsele de program, precum și altor persoane fizice și juridice (consultanți, experți, stagiați, etc.).

10. Fiecare utilizator autorizat al sistemelor, echipamentelor și produselor de program ale Ministerului Economiei și Infrastructurii poartă răspundere personală pentru aplicarea întocmai în activitatea sa a regulamentelor și procedurilor de securitate cibernetică în vigoare, elaborate și aprobate, conform standardelor internaționale, legislației naționale, legislației speciale și a reglementărilor interne de funcționare. De asemenea, orice utilizator autorizat al sistemelor, echipamentelor și produselor de program are obligația raportării oricărui incident de securitate.

11. Nerespectarea Politicii interne privind securitatea cibernetică a Ministerului Economiei și Infrastructurii atrage după sine aplicarea măsurilor disciplinare, precum și revizuirea drepturilor de acces la informație.

12. Politica internă privind securitatea cibernetică a Ministerului Economiei și Infrastructurii este revizuită anual în vederea actualizării și adaptării la noile condiții și cerințe.