Ministerul Mediului
I.P. „Oficiul Național de Implementare a Proiectelor în domeniul Mediului”

O R D I N
nr. 125 din „12” august 2024

Cu privire la aprobarea și punerea în aplicare a Politicii de securitate cibernetică Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului"

În scopul asigurării respectării Cerințelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017, precum și executării prevederilor art.10 alin.(1) și art.18 alin.(1) din Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat, cu modificările ulterioare, art.11 alin.(2) lit. e) și f) și art.24 din Legea nr.711/2007 cu privire la registre, cu modificările ulterioare, și ale Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărârea Guvernului nr.811/2015, în temeiul pct.7, subpct. 10), pct. 8 subpct 6) și 14), precum și în conformitate cu prevederile Statutului Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului” aprobat prin Hotărârea Guvernului nr. 1249/2018.

O R D O N:

1. Se aprobă Politica de securitate cibernetică a Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului", conform Anexei;

2. Prezentul Ordin se aduce la cunoștință tuturor angajaților și persoanelor contractate a Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului";

3. Controlul executării prezentului Ordin mi-l asum.

Director interimar **Nicolae ARNĂUT**

„APROBAT"
Director interimar al I.P.„ ONIPM"

/_____/ Nicolae ARNĂUT

POLITICA INTERNĂ PRIVIND SECURITATE CIBERNETICĂ ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE I.P. „OFICIUL NAȚIONAL DE IMPLEMENTARE A PROIECTELOR ÎN DOMENIUL MEDIULUI"

Politica internă privind securitatea cibernetică a Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului"

1. Introducere

Acest regulament stabilește cerințele și măsurile necesare pentru asigurarea securității cibernetice în cadrul Instituției Publice „Oficiul Național de Implementare a Proiectelor în domeniul Mediului".

Scopul principal este protecția sistemelor, rețelelor și informațiilor împotriva accesului neautorizat, atacurilor cibernetice și altor riscuri precum și asigurarea integrității, confidențialității și disponibilității informației, precum și asigurarea colectării, procesării, stocării și accesării în siguranță a datelor, datelor cu caracter personal, inclusiv a datelor de interes public.

2. Noțiuni și definiții

Informație – Totalitatea datelor publice și închise/secrete aferente instituției.
Securitatea informațională – Ansamblu de activități pentru protejarea informației împotriva amenințărilor.
Autentificare multifactorială – Autentificare cu cel puțin doi factori independenți.
Firewall (Paravan de protecție) – Dispozitiv configurat pentru a filtra traficul între domenii de securitate.
Phishing – Atac cibernetic pentru a obține informații confidențiale.
Programe malware (software rău intenționat) reprezintă o aplicație sau script conceput cu scopul de a provoca modificarea sau ștergerea datelor informatice, deteriorarea, restricționarea sau asigurarea accesului neautorizat/ilegal la calculatoare sau rețele.
VPN – Rețea virtuală privată ce oferă o conexiune criptată și securizată.

3. Domeniul de aplicare

Regulamentul se aplică tuturor angajaților, colaboratorilor și terților care au acces la resursele informaționale ale instituției, echipamente (hardware), produse de program (software) și sistemele informatice aflate în diverse stadii de elaborare, testare și implementare.

Prevederile Regulamentului se respectă și se aplică nediscriminatoriu de către toate persoanele ce activează sau interacționează cu acesta în cadrul Instituției, cărora li s-a autorizat accesul la sistemele, echipamentele și produsele de program.

4. Cadrul legal

Regulamentul se bazează pe actele normative ale Republicii Moldova:

Hotărârea Guvernului nr. 201/2017 privind cerințele minime de securitate cibernetică. Legea nr. 467 din 2003 privind informatizarea și resursele informaționale de stat.

Alte reglementări relevante în domeniul securității cibernetice.

5. Principii de bază

Confidențialitate – Accesul la informații este permis doar persoanelor autorizate. Integritate: Asigurarea acurateței și completitudinii informațiilor.

Disponibilitate – Informațiile și sistemele sunt accesibile atunci când este necesar.

Non-repudiere – Asigurarea că expeditorul/destinatarul nu poate nega transmiterea/recepționarea informațiilor.

6. Scopuri și obiective

Regulamentul cu privire la securitatea cibernetică (în continuare Regulament) a I.P. "Oficiul

Național de Implementare a Proiectelor în domeniul Mediului" (în continuare Instituție) 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.

Scopul regulamentului include următoarele obiective:

- Respectarea cadrului legislativ-normativ național și internațional.
- Implementarea procedurilor și măsurilor de securitate cibernetică.
- Prevenirea accesului neautorizat la sistemele instituției.
- Asigurarea continuității și securității sistemelor informaționale.
- Intervenție promptă și eficientă în cazul incidentelor de securitate.
- Sporirea calificării angajaților în domeniul securității cibernetice.
- Gestionarea riscurilor cibernetice și sporirea nivelului de protecție.

7. Responsabilități

Responsabilul de securitate cibernetică este desemnat de directorul Instituției și este responsabil de implementarea, monitorizarea și actualizarea măsurilor de securitate.

Angajații: Respectă regulile și politicile și raportează orice incident de securitate.

8. Reguli de bază ale securității cibernetice

8.1. Controlul accesului

Drepturile de administrare sunt atribuite persoanei responsabile din cadrul Instituției.

Divizarea rolurilor de administrator și utilizator în conturile stațiilor de lucru și la resursele informaționale deținute de instituție.

Fiecărui angajat sau persoane ce prestează servicii în folosul Instituției (stagiar, expert etc.) la numirea în funcție (la începutul contractului de stagiu, prestări servicii etc.) vor fi atribuite conturi personalizate de acces la resursele informaționale ale Instituției..

Accesul la informații este atribuit în funcție de atribuțiile funcționale.

Gestionarea parolelor se efectuează conform HG201/2017.

8.2. Securitatea echipamentelor

Securitatea stațiilor de lucru: Rolurile de administrator și utilizator sunt separate; instalarea de aplicații este restricționată; se folosește antivirus licențiat și se realizează copii de rezervă.

Securitatea Rețelelor: Modificarea obligatorie a credențialelor de acces implicite a echipamentelor de rețea; se utilizează protocoale și echipamente securizate; Filtrarea echipamentelor permise pe baza adresei fizice(MAC). Ascunderea identificatorului rețelei wireless(SSID). Divizarea rețelei interne de rețeaua oaspeților. Monitorizarea permanentă a rețelelor.

Securitatea Serverelor: În conformitate cu Hotărârea Guvernului 414 din 2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, securitatea fizică a serverelor alocate Instituției este asigurată de I.P. „Serviciul Tehnologia Informației și Securitatea Cibernetică"; Accesul la servere se face doar prin rețeaua Guvernamentală sau VPN.

8.3. Analiza riscurilor

Identificarea riscurilor: Se documentează riscurile ce pot afecta integritatea datelor.

Evaluarea impactului: Riscurile sunt evaluate și prioritizate.

Plan de răspuns: Se elaborează un plan pentru remedierea riscurilor.

Registrul riscurilor: Se documentează riscurile, planul de răspuns și monitorizarea acestora.

9. Măsuri de Securitate

9.1. Măsuri organizaționale - Implementarea regulilor interne privind accesul la resurse. Instruirea periodică a personalului.

9.2. Măsuri tehnice - Utilizarea de software antivirus și firewall. Criptarea datelor sensibile. Implementarea autentificării multifactoriale.

9.3. Măsuri fizice - Controlul accesului fizic la servere și echipamente IT.

10. Organizarea procesului intern de securitate cibernetică

Conducerea instituției este responsabilă pentru asigurarea unei abordări adecvate la nivel instituțional.

Angajatul responsabil de securitate cibernetică este responsabil de instruirea personalului și punerea în aplicare a sistemului de management al securității cibernetice în Instituție, 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 asigurată;
3) integritatea informațiilor este asigurată;
4) disponibilitatea informațiilor, serviciilor și sistemelor este asigurată la necesitate;
5) cerințele și obiectivele organizaționale sunt îndeplinite;
6) cerințele legislative și de reglementare sunt îndeplinite;

11. Gestionarea riscurilor și incidentelor

Evaluare periodică a riscurilor cibernetice. Stabilirea unei proceduri clare pentru gestionarea incidentelor de securitate. Elaborarea și implementarea unui plan de continuitate a activității.

12. Monitorizare și audit

Monitorizare continuă a activităților în rețea pentru a detecta activități suspecte. Organizarea de audituri periodice pentru evaluarea conformității cu regulamentul.

Pentru implementarea eficientă a politicii interne de securitate cibernetică, instituția va desfășura anual un audit intern de securitate cibernetică care va avea următoarele obiective principale:

1) **Evaluarea vulnerabilităților și riscurilor:** Se va identifica și analiza amenințările relevante asupra resurselor informaționale și sistemelor IT. Vor fi determinate amenințările care trebuie eliminate și cele care pot fi tolerate, iar probabilitatea producerii acestora și impactul potențial vor fi evaluate în mod detaliat. De asemenea, se va realiza ierarhizarea riscurilor, ținând cont de gravitatea și urgența acestora.

2) **Identificarea sistemelor și echipamentelor critice:** Se vor identifica sistemele informatice, echipamentele și produsele software care necesită protecție sporită, determinând nivelul adecvat de securitate necesar pentru fiecare.

3) **Stabilirea măsurilor de securitate:** Vor fi analizate și selectate mijloacele adecvate pentru implementarea măsurilor de securitate cibernetică, în conformitate cu cerințele legislative și standardele internaționale în domeniu.

13. Sancțiuni

Nerespectarea regulamentului poate duce la sancțiuni disciplinare, inclusiv restricționarea accesului la resursele informaționale.

14. Formare și conștientizare

Organizarea de sesiuni de formare pentru angajați privind securitatea cibernetică. Campanii periodice de informare despre riscurile cibernetice.

15. Revizuirea și actualizarea regulamentului

Regulamentul va fi revizuit anual sau ori de câte ori este necesar pentru a reflecta modificările legislative sau schimbările în infrastructura IT a instituției.