Anexă
la Hotărîrea Consiliului de Supraveghere
al Băncii Naționale a Moldovei
Nr. 22 din 27 iulie 2020

Politica de securitate a informației a Băncii Naționale a Moldovei

I. Declarația politicii

1. Informația este un bun de mare valoare pentru Banca Națională a Moldovei (BNM) în intenția sa de a-şi îmbunătăți continuu activitatea şi de a atinge obiectivele stabilite în cadrul legal aplicabil activității BNM.

2. Comitetul Executiv al BNM (CE) urmează să asigure capacitatea BNM de a gestiona securizat toată informația din cadrul BNM indiferent de forma ei (electronică, pe suport de hîrtie, comunicată orală). În acest scop, CE în limitele responsabilităților atribuite și angajamentelor asumate va susține implementarea și menținerea unui cadru intern aferent securității informației și cibernetice capabil de a asigura protecția sistemului informațional (SI) al BNM contra amenințărilor posibile de securitate.

II. Obiectivele politicii

3. Obiectivul primar al politicii de securitate a informației a BNM (în continuare Politică) este de a stabili contextul organizațional de nivel general care să asigure atingerea obiectivelor cu privire la asigurarea securității informației și securității cibernetice în cadrul BNM.

4. Alte obiective ale politicii sunt de a asigura gestionarea securizată a informației în cadrul SI al BNM și de a minimiza impactul ce poate apărea ca rezultat al incidentelor de securitate.

III. Domeniul de aplicare

5. Prezenta politică se aplică asupra tuturor angajaților BNM şi asupra tuturor terțelor părți ce interacționează cu BNM, prin introducerea clauzelor privind securitatea informației și securitatea cibernetică în cadrul contractelor de prestare a serviciilor sau a altor tipuri de contracte încheiate de terți cu BNM.

IV. Termeni şi definiții

Cadru intern aferent securității informației și cibernetice – totalitatea reglementărilor interne, a proceselor și structurilor organizatorice stabilite în cadrul BNM, ce asigură gestionarea adecvată a riscurilor aferente securității informației și cibernetice.

Confidențialitate – proprietatea informației de a fi disponibilă doar persoanelor sau proceselor autorizate să aibă acces la ea.

Integritate – proprietatea informației de a fi exactă, completă și coerentă la nivelul diferitor sisteme TIC.

Disponibilitate – proprietatea informației de a fi disponibilă şi utilizabilă la cererea unei persoane sau unui proces autorizat.

Resursă informațională – orice bun material sau nematerial al BNM necesar gestiunii informației (ex.: date, aplicații, echipamente de calcul, alte elemente de infrastructură).

Securitatea informației – asigurarea confidențialității, disponibilității informației şi protejarea integrității informației, în orice formă a sa (electronică, pe suport hârtie, etc.).

Securitatea Cibernetică – asigurarea securității Tehnologiei Informației și a Comunicațiilor (TIC) și protejarea acestora împotriva accesului neautorizat.

Risc de securitate a informației – probabilitatea ca un anumit eveniment se va realiza și va avea impact advers asupra confidențialității, integrității sau disponibilității informației aferent proceselor de activitate.

Risc aferent tehnologiei informației şi comunicațiilor (risc TIC) – subcategorie a riscului operațional care se referă la riscul de pierdere/impact negativ, din cauza compromiterii confidențialității informațiilor, integrității datelor, aferent sistemelor informaționale,

indisponibilității sistemelor informaționale şi/sau a datelor, precum şi incapacitatea de a schimba TIC într-o anumită perioadă şi la un cost rezonabil.
Gestiunea riscului –proces continuu și sistematic, cu responsabilități stabilite în reglementări interne, de identificare, evaluare/măsurare, monitorizare și aplicarea măsurilor pentru controlul sau atenuarea expunerii la risc.
Măsură de securitate – mijloc de reducere a nivelului riscului de securitate prin diminuarea probabilității sau a impactului acestuia.

V. Principiile de realizare a politicii de securitate

6. În scopul atingerii obiectivelor Politicii se vor aplica consecvent următoarele principii:
Responsabilitatea –asigurarea securității informației trebuie să fie clar stabilită şi, după caz acceptată contractual. Aplicarea acestui principiu semnifică şi faptul că pentru toate acțiunile importante aferente informației şi resurselor informaționale va fi posibilă stabilirea responsabilului. Responsabilitatea se stabilește, în reglementările interne, pentru toate nivelele ierarhice, inclusiv membrilor organelor de conducere a BNM, conducătorilor de subdiviziuni, angajaților şi anumitor funcții specifice;
Instruirea – toate părțile implicate ce dețin atribuții de asigurare a securității informației și cibernetice, trebuie să fie suficient instruite pentru a cunoaște atribuțiile deținute și amenințările de securitate aferente domeniilor de responsabilitate proprii;
Proporționalitatea – măsurile de securitate elaborate și aplicate trebuie să fie proporționale nivelului riscurilor;
Promptitudinea – toți cei responsabili trebuie să reacționeze în timp util şi într-o manieră coordonată pentru a preveni sau a răspunde la amenințările şi incidentele de securitate a informației;
Eficacitatea – eficacitatea procesului de asigurare a securității informației trebuie să fie evaluată cu regularitate în baza unor indicatori predefiniți.

VI. Roluri şi responsabilități

7. Membrii Consiliului de Supraveghere, membrii Comitetului Executiv, și orice angajat al Băncii Naționale a Moldovei indiferent de funcția deținută este obligat să asigure securitatea informației aflate în posesia sa și la care are acces, oricare ar fi forma ei. Totodată, pentru realizarea obiectivului politicii de securitate în cadrul BNM, se stabilesc în particular următoarele roluri și responsabilități:
8. Comitetul executiv aprobă reglementarile interne care pun în aplicare Politica.
9. Conducătorii de subdiviziune:

a) asigură gestionarea adecvată a riscurilor TIC și de securitate a informației în cadrul proceselor de activitate ale căror proprietar este subdiviziunea;
b) asigură informarea angajaților din subordine cu privire la reglementările de securitate a informației;
c) asigură oferirea accesului angajaților la resursele informaționale a căror proprietar sunt în strictă conformitate cu îndeplinirea funcțiilor de serviciu;
d) asigură, în coordonare cu OSI, includerea clauzelor privind securitatea informației și securitatea cibernetică în contractele încheiate cu terțele părți cu care interacționează subdiviziunea sa şi care au acces la informația din cadrul BNM.

10. Ofițerul de securitate a informației (OSI), care este numit prin ordinul guvernatorului BNM:

a) elaborează şi coordonează implementarea Politicii şi standardelor de securitate a informației și securitate cibernetică în cadrul BNM;

b) monitorizează respectarea prevederilor reglementărilor interne privind securitatea informației și securitatea cibernetică în cadrul BNM, şi întreprinde măsuri de rigoare în cazul încălcării lor;
c) identifică deficiențe și amenințări ce generează riscuri TIC și de securitate a informației în cadrul proceselor existente şi coordonează măsurile de înlăturare a acestora;
d) contribuie la buna cooperare cu alte autorități ale statului în domeniul securității informației;
e) asigură transfer de cunoștințe prin instruirea angajaților în domeniul securității informației;
f) inițiază investigații interne în cadrul BNM cu privire la încălcarea cadrului normativ sau a reglementărilor interne de asigurare a securității informației și cibernetice de către angajații BNM.

11. Proprietar al informației / resursei informaționale se determină ca fiind cea mai potrivită subdiviziune, considerând importanța informației / resursei informaționale în cadrul activității subdiviziunii şi necesitatea subdiviziunii de a controla informația / resursa informațională. Responsabilitățile Posesorului informației / resursei informaționale:

a) stabilește cerințele de securitate aferente resurselor a cărui posesor este și selectează mijloace de securitate corespunzătoare nivelului riscurilor. În acest scop, Posesorul informației / resursei informaționale poate solicita suportul Gestionarului informației / resursei informaționale și a OSI;
b) acordă şi/sau autorizează accesul la informațiile / resursele informaționale din posesia sa, revizuiește regulat drepturile de acces.

12. Gestionar al informației / resursei informaționale în cadrul BNM poate fi orice subdiviziune de sine stătătoare a BNM. Gestionarul se determină conform responsabilităților subdiviziunii în cadrul BNM. În cazul resurselor informaționale ce țin de tehnologiile informaționale, gestionarul resurselor este departamentul responsabil de tehnologii informaționale. Responsabilitățile Gestionarului includ:

a) gestionează informația şi resursa informațională conform reglementărilor interne de asigurare a securității informației și cibernetice;
b) implementează măsurile şi soluțiile de securitate care să corespundă cerințelor de securitate ale Proprietarului. Oferă suportului necesar Proprietarului în scopul asigurării gestiunii adecvate a riscurilor TIC și de securitate a informației.

13. Utilizatori sunt angajații BNM ce accesează informația în scopul exercitării atribuțiilor de serviciu. Utilizatorii:

a) respectă normele şi prevederile aferente securității informației în cadrul BNM;
b) manifestă o atitudine responsabilă şi prudentă la accesarea informației, utilizarea informației și resurselor informaționale ale BNM, asigurând securitatea informației și cibernetică în cadrul activităților desfăşurate.

VII. Ordinea de revizuire

14. Politica va fi revizuită periodic, ca rezultat al apariției modificărilor în ceea ce privește rolurile și responsabilitățile în cadrul BNM, dar nu mai rar de o dată la 3 ani.