

## **Politica BC „Moldova Agroinbank” S.A privind securitatea informațională**

### **Pornind de la:**

- intențiile băncii de a-și consolida și în continuare pozițiile de lider pe piața financiar-bancară, de a se menține ca o instituție cu cele mai înalte standarde de securitate;
- responsabilitățile pe care banca și le-a asumat față de acționari, clienți și parteneri de afaceri;
- conformarea băncii la cerințele legislației Republicii Moldova și actelor normative de rigoare, standardelor naționale și internaționale în domeniul securității informaționale;
- implementarea în bancă a sistemelor informatice principal noi, bazate pe tehnologiile informaționale moderne, cum ar fi deservirea bancară de la distanță cu utilizarea tehnologiilor Internet;
- includerea în procesul de interacțiune informațională cu banca a unui număr tot mai mare de personal;
- tendințele accentuate de sporire în activitățile desfășurate de bancă a necesităților informaționale și a volumului schimbului de informație cu partenerii de afaceri și instituțiile statale;
- existența multiplelor pericole și perfecționarea continuă a metodelor și canalelor de penetrare a sistemelor informatice cu intenții frauduloase;
- conștientizarea necesității protejării oricăror resurse informaționale (tehnologii, sisteme de prelucrare și transmitere a informației, baze de date etc.);
- recunoașterea și acceptarea drept călăuză a principiilor de transparență în activitate și în relații.

Banca **declară următoarele intenții privind securitatea informațională**, pe care le va urma cu consecvență și le va realiza cu insistență:

- aplicarea sistemului de management al securității informaționale al băncii, cu menținerea certificatului de conformitate cu Standardul Internațional de Securitate Informațională ISO 27001:2005, obținut în anul 2009, prin îmbunătățirea continuă a sistemului în corespundere cu cerințele de afaceri ale băncii și legislația în vigoare;
- protejarea consecventă a confidențialității, integrității și disponibilității informației existente sub diferite forme, proprie atât băncii cât și clienților ei;
- protejarea sistemelor informaționale ale băncii de orice acces neautorizat atât din interiorul, cât și din exteriorul băncii, precum și de orice amenințări, care ar afecta disponibilitatea lor;
- asigurarea aplicării sistemelor informaționale ale băncii, care vor garanta:
  - 2 integritatea sistemului contabil și financiar;
  - 3 oportunitatea raportării financiar-contabile în procesul guvernării corporative în bancă;
- efectuarea o data pe an a analizei riscurilor informaționale pentru bunurile informaționale critice, urmată de elaborarea și implementarea măsurilor necesare pentru reducerea riscurilor constatate;
- menținerea riscurilor informaționale la nivelul acceptat de managementul băncii;
- actualizarea Planului de continuitate a afacerii cel puțin o data pe an sau mai des, în cazurile schimbărilor semnificative, pentru a asigura în permanență actualitatea și eficiența lui ;
- definirea responsabilităților generale și individuale pentru administrarea securității informaționale în bancă, inclusiv raportarea trimestrială a incidentelor de securitate;
- actualizarea cel puțin o data pe an a politicilor și procedurilor de securitate informațională, adoptate în bancă, asigurând menținerea unui sistem eficient de instruire permanentă și continuă a salariaților și clienților băncii pe acest domeniu;
- asigurarea protecției și bunăstării salariaților băncii;
- raportarea promptă a incidentelor de securitate, care au avut loc și utilizarea tuturor posibilităților, pentru investigarea și lichidarea operativă a consecințelor lor;
- sancționarea încălcării politicilor și procedurilor de securitate informațională conform legislației în vigoare, inclusiv prin:
  - 4 desfacerea contractului de muncă (în cazul salariaților băncii);
  - 5 rezilierea contractului (în cazul clienților băncii, consultantților sau altor părți terțe);
- raportarea organelor competente privind acțiunile, care contravin legislației în vigoare.