

## Condiții de utilizare a sistemului „MAIBank”

### 1. Prevederi generale

- 1.1.** BC „Moldova – Agroindbank” S.A. (în continuare „Banca” sau „MAIB”), furnizorul, publică următoarele Condiții de utilizare a Sistemului „MAIBank” (în continuare „Condiții”).
- 1.2.** Prezentele Condiții descriu modul în care Banca oferă persoanelor fizice posibilitatea utilizării Sistemului „MAIBank”.
- 1.3.** Banca își rezervă dreptul de a modifica unilateral aceste condiții, informând despre aceasta Utilizatorul cu cel puțin 2 luni până la data intrării în vigoare a acestora, prin plasarea Condițiilor pe pagina web [www.maib.md](http://www.maib.md), precum și în cadrul aplicației MAIBank. Prin acceptarea utilizării sistemului „MAIBank” Utilizatorul își exprimă în mod expres și irevocabil acordul său privind acceptarea prezentelor Condiții și a dreptului Băncii de a modifica în mod unilateral Condițiile.
- 1.4.** În cazul în care utilizatorul este Client, prezentele Condiții completează și detaliază relația între Utilizator și Bancă, stabilită în conformitate cu Condițiile Standard din Contractul de cont curent bancar pentru persoane fizice. Condițiile Standard din Contractul de cont curent bancar pentru persoane fizice sunt puse la cunoștința fiecărui Client în momentul semnării Contractului de cont curent bancar pentru persoane fizice și sunt accesibile pe pagina web a Băncii.
- 1.5.** Utilizator al sistemului „MAIBank” poate fi orice persoană fizică (pentru Zona Publică) sau Client persoană fizică titular al contului bancar deschis la Bancă (pentru Zona Privată).
- 1.6.** Sistemul „MAIBank” este o aplicație mobilă creată pentru sistemele de operare Android și iOS.
- 1.7.** Serviciile sistemului „MAIBank” sunt disponibile Utilizatorilor pentru accesare și utilizare 24/24 ore, 7/7 zile.
- 1.8.** Pentru navigarea în sistemul „MAIBank”, Banca nu va percepe comisioane, acces la sistem fiind oferit Utilizatorilor în mod gratuit.
- 1.9.** Comisioanele pentru utilizarea serviciilor electronice integrate în aplicație (P2P, T2C, Mobile Banking) se vor percepe în conformitate cu Registrul tarifelor la produsele și serviciile bancare oferite clienților în vigoare la data utilizării serviciilor în cauză.
- 1.10.** Pentru informații suplimentare despre sistemul „MAIBank”, utilizatorii poate accesa pagina WEB a Băncii sau apela la numărul de telefon /+373/ 22 450 603.

### 2. Noțiuni utilizate

- 2.1.** Noțiunile utilizate în prezentul document au următoarele sensuri:

- 2.1.1. Autentificare** – procedura care permite Băncii să verifice identitatea unui Utilizator sau valabilitatea utilizării unui anumit instrument de plată, inclusiv utilizarea elementelor de securitate personalizate ale Utilizatorului;

În cadrul Sistemului sunt aplicate următoarele tipuri de autentificare:

- a. **Logare** – Utilizatorul va introduce numărului cardului și parola de acces setată la etapa activării profilului (numită în continuare „PIN5”). În următorul ecran va introduce codul OTP primit prin SMS la numărul de telefon al Clientului existent în baza de date a Băncii;

**[Public]**

- b. **Deblocarea aplicației prin parola standard - PIN5** – Utilizatorul va debloca aplicația în intervalul unei sesiuni (de la Logare până la Ieșire) prin introducerea parolei de acces dedicate - PIN5 (cod static compus din 5 cifre) setată la etapa activării profilului;
  - c. **Deblocarea aplicației prin metoda telefonului** – Utilizatorul va debloca aplicația în intervalul unei sesiuni (de la Logare până la Ieșire) utilizând parola de acces setată la etapa activării profilului sau autentificarea biometrică încorporată în dispozitiv (citire amprentă digitală, recunoaștere față sau voce). metoda de deblocare setată în telefonul Clientului, aceasta poate fi o parolă (cod numeric), desen pe ecran sau autentificarea biometrică încorporată în dispozitiv (citire amprentă digitală, recunoaștere față sau voce). La această etapă Clientul poate alege să deblocheze aplicația prin PIN5. Aceeași posibilitate va fi oferită de către aplicație în cazul deblocării nereușite prin metoda telefonului.
- 2.1.2. **Autentificare de tip SMS OTP** – tipul autentificării, care prevede transmiterea de către Bancă în adresa Utilizatorului a unei Parole de Unică Folosință;
  - 2.1.3. **Client al Băncii/ Client** – titular al contului(urilor) bancar(e) deschis(e) în Bancă;
  - 2.1.4. **One Time Password/ Parolă de Unică Folosință/ OTP** – cod alfanumeric, generat de sistemul informațional al Băncii în mod aleatoriu, transmis Utilizatorului și care este utilizat în cadrul MAIBank în calitate de cod de autentificare și autorizare pentru efectuarea Tranzacțiilor.
  - 2.1.5. **Parolă de acces** – cod alfanumeric, generat de Sistem, care este utilizat în calitate de cod de autentificare a Utilizatorului la conectarea acestuia la Sistem. Tipul Parolei de acces poate fi modificat doar de către Utilizator și doar după autentificare în Sistem.
  - 2.1.6. **Profil al utilizatorului** – configurație a contului Utilizatorului în Sistem, care conține date de identificare asociate unui Utilizator în cadrul Sistemului.
  - 2.1.7. **Serviciul P2P** – serviciu care oferă posibilitatea Utilizatorului de a efectua transferul mijloacelor bănești din cardul propriu, emis de Bancă, de tip Visa sau Mastercard la un alt card VISA sau Mastercard, inclusiv transferuri de la carduri AMEX, VISA sau MasterCard emise de Bancă la carduri AMEX emise de Bancă;
  - 2.1.8. **Serviciul T2C** – serviciu care oferă posibilitatea beneficiarilor de remitențe de a transfera mijloacele bănești primite prin sisteme de remiteri de bani direct la cardul propriu deschis în Bancă;
  - 2.1.9. **Sistemul MAIBank/ Sistem/ aplicația MAIBank/ aplicație mobilă MAIBank/ serviciul MAIBank** – Sistem ADD de tip mobile payments, prin intermediul căruia Utilizatorul, de la un telefon mobil tip smartphone sau tabletă conectat la rețeaua Internet, poate efectua Tranzacții, vizualiza situația conturilor sale bancare etc.
  - 2.1.10. **Sistem automatizat de deservire la distanță/ Sistem ADD** – soluție informatică, pusă la dispoziție de către Bancă clientului său, ce permite acestui client prin intermediul unei aplicații informatice, a unei metode de autentificare și al unui mijloc de comunicație să aibă acces de la distanță la mijloacele aflate în contul de plăți al clientului în scopul: obținerii de informații privind starea contului de plăți și a Tranzacțiilor realizate, efectuării Tranzacțiilor în numele și la ordinul clientului din contul mijloacelor aflate în contul de plăți.
  - 2.1.11. **Tranzacție** – operațiune de plată efectuată în formă electronică prin intermediul Sistemului ADD, utilizând un mecanism ce permite verificarea autenticității, integrității și nonrepudierii acesteia.

**[Public]**

- 2.1.12. **Utilizator** – orice persoană fizică, care a instalat cu succes aplicația MAIBank în telefonul său mobil și a acceptat Condițiile de utilizare a sistemului „MAIBank” afișate în interfața MAIBank, prin apăsarea butonului „accept”.
- 2.1.13. **Zona de acces MAIBank, fără autentificare/Zona Publică** – reprezintă parte a funcționalităților aplicației MAIBank, care vor fi accesibile Utilizatorilor, fără autentificare cu Parolă de acces (serviciile P2P, T2C, etc.).
- 2.1.14. **Zona de acces MAIBank, cu autentificare/Zona Privată** – reprezintă parte a funcționalităților aplicației MAIBank, care vor fi accesibile Utilizatorilor după respectarea următoarelor condiții:
- a) Sistem zona privată este oferit oricărui client al Băncii, care este titular al unui cont de card bancar deschis la MAIB, dar și care deține informații actualizate a profilului său în sistemul informatic al băncii (număr de telefon mobil al unui operator de telefonie mobilă din Republica Moldova, veridic și actualizat).
  - b) Pentru a avea acces la zona privată, utilizatorul va parcurge în mod obligatoriu procedura de activare a profilului. Aceasta presupune autentificare după o serie de date personale și parola de unică folosință OTP.

### **3. Modul de conectare și utilizare a sistemului „MAIBank”**

**3.1.** Accesul la funcționalitățile aplicației mobile ”MAIBank” din Zona Publică este oferit Utilizatorilor la distanță, conform prezentelor Condiții, fără a fi necesară depunerea unei solicitări de abonare la sucursalele Băncii.

**3.2.** Accesul la funcționalitățile aplicației mobile ”MAIBank” din Zona Privată este oferit Clienților la distanță, conform Condițiilor Standard din Contractul de cont curent bancar pentru persoane fizice și în corespundere cu prezentele Condiții, fără a fi necesară depunerea unei solicitări de abonare la sucursalele Băncii.

**3.3.** Utilizarea Zonei Publice a sistemului „MAIBank” va fi posibilă doar după acceptarea de către Utilizator a prezentelor Condiții.

**3.4.** Utilizarea Zonei Private a sistemului „MAIBank” va fi posibilă doar după acceptarea de către Utilizator a prezentelor Condiții și indicarea corectă a parolei de acces tip OTP.

**3.5.** Funcționalitățile aplicației MAIBank sunt delimitate în interfața aplicației MAIBank după principul obligativității Autentificării Utilizatorului în Sistem, serviciile oferite fiind grupate în următoarele **zone**:

3.5.1. **Zona Publică**, care conține următoarele servicii

- a) *Tranzacționale* – transferuri de tip P2P și T2C;
- b) *Informaționale* – harta punctelor, contacte, materiale promoționale ale Băncii;

3.5.2. **Zona Privată**, care conține următoarele servicii:

- a) *Tranzacționale* – transfer între carduri proprii emise de MAIB în monedă națională și valută străină, achitarea serviciilor prestatorilor de servicii, transferuri de tip P2P, T2C, Cash by Code și altele.
- b) *Informaționale* – vizualizarea soldului contului/cardului, vizualizarea extraselor de cont, vizualizarea graficelor la credite și depozite, vizualizarea istoricului tranzacțiilor, afișarea cursului de schimb valutar etc.

**3.6.** Modalitatea de conectare la Zona Privată (logarea) este după cum urmează:

- a) Utilizatorul lansează aplicația „MAIBank” Zona Publică și apasă butonul „Intră” ;

**[Public]**

- b) În pagina de logare Utilizatorul selectează opțiunea „Ai uitat parola sau te loghezi prima oară”;
- c) În următorul ecran introduce numărul cardului său bancar activ, emis de MAIB;
- d) Introduce data de expirare a cardului;
- e) Introduce codul său fiscal (IDNP);
- f) Primește OTP;
- g) Introduce OTP-ul primit pentru autentificare și confirmare;
- h) În următorul ecran setează o parolă de acces la aplicație compusă din 5 cifre (PIN5);
- i) Selectează metoda de accesare a aplicației MAIBank în cadrul unei sesiuni active de lucru: modalitatea de bază va fi utilizând PIN5 sau modalitatea de deblocare a telefonului (biometrie, desen pe ecran ș.a.) păstrând și posibilitatea accesului cu PIN5;
- j) În următorul ecran Utilizatorul are posibilitatea (opțional) să seteze opțiunea „Fii vizibil” care îi va permite să primească transferuri P2P efectuate de alți Utilizatori ai aplicației MAIBank doar după numărul său de telefon din lista de contacte a acestora;
- k) În următorul ecran Utilizatorul are posibilitatea (opțional) să vizualizeze descrierea succintă a funcționalităților de bază ale aplicației (în cadrul instrucțiunii proces);
- l) Primește acces la Profilul personal.

**3.7.** Zona Publică va fi disponibilă Utilizatorilor spre utilizare prin instalarea acesteia pe telefon sau tabletă cu sistem de operare Android sau iOS.

**3.8.** Aplicația urmează a fi descărcată din Google Play sau Apple Store, utilizând criteriul de căutare sintagma ”MAIBank”.

**3.9.** Cerințele minime față de echipamentul tehnic pentru a utiliza aplicația MAIBank: Clientul trebuie să dispună de un telefon/tabletă cu sistem de operare Android (începând cu versiunea indicată pe platforma „Play Store”) sau iOS (începând cu versiunea indicată pe platforma „App Store”) cu conexiune la rețeaua Internet.

**3.10.** Banca oferă acces la funcționalitățile și serviciile aplicației, iar Utilizatorul este responsabil de utilizarea corespunzătoare a echipamentului tehnic (telefon/tabletă) și asigurarea confidențialității utilizării elementelor de identificare utilizate pentru accesarea serviciilor oferite de Bancă.

**3.11.** Pentru autorizarea Tranzacțiilor efectuate în Sistem se va utiliza OTP.

**3.12.** Modificarea Profilului utilizatorului se efectuează prin următoarele modalități:

3.13.1. în baza Cererii de modificare a datelor personale depusă de Utilizator în reprezentanțele Băncii pentru:

- a) modificarea numărului de telefon al Utilizatorului;
- b) modificarea numelui Utilizatorului.

3.13.2. de către Utilizator în aplicație pentru:

- c) modificarea PIN5;
- d) modificarea limbii de comunicare utilizate la expedierea notificărilor cu privire la statutul Tranzacțiilor sau la expedierea OTP.

**3.13.** Dezactivarea Utilizatorului de la Sistem poate fi efectuată precum urmează:

- 3.13.1. de către Utilizator din aplicație, accesând meniul principal, secțiunea “Setări”> “Dezactivarea profilului”, cu confirmarea intenției prin introducerea codului OTP;

[Public]

3.13.2. de către Bancă la solicitarea Utilizatorului prin contactarea Serviciului Contact Center al Băncii, care va executa dezactivarea Utilizatorului (blocarea) de la sistemul MAIBank;

#### **4. Prelucrarea datelor cu caracter personal**

**4.1.** Datele cu caracter personal, prelucrate în cadrul sistemului “MAIBank”, sunt tratate în conformitate cu prevederile legislației în vigoare și normelor internaționale aplicabile, care reglementează protecția datelor cu caracter personal. Banca este înregistrată în calitate de operator de date cu caracter personal, cu numărul 0000144, la Centrul Național pentru Protecția Datelor cu Caracter Personal.

**4.2. Scopul prelucrării datelor cu caracter personal** în cadrul sistemului “MAIBank” constă în oferirea produselor/serviciilor prestate de către Bancă prin intermediul aplicației mobile “MAIBank” pentru Utilizatori.

**4.3. Temeiul legal** de prelucrare a datelor cu caracter personal de către Bancă îl constituie obligația legală care îi revine Băncii conform legislației cu privire la activitatea băncilor (Legea privind activitatea băncilor, nr.202 din 06.10.2017), legislației privind prevenirea spălării banilor și finanțării terorismului (Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului nr. 308 din 22.12.2017), precum și, în cazul Clienților, obligația de executare a prevederilor contractuale la care Banca este parte (contractul de cont curent bancar pentru persoane fizice și contractul privind emiterea și utilizarea cardurilor de către persoanele fizice, încheiate cu Clienții).

**4.4. Subiecții datelor cu caracter personal**, sunt Utilizatorii, precum și beneficiarii efectivi identificați în cadrul serviciilor prestate prin intermediul sistemului “MAIBank”.

**4.5. În cadrul sistemului “MAIBank” sunt prelucrate următoarele categorii de date cu caracter personal:**

- 4.5.1. *date de identificare*: nume, prenume, codul numeric personal (IDNP);
- 4.5.2. *date de contact*: număr de telefon mobil, adresa de poștă electronică;
- 4.5.3. *date bancare*: conturi bancare, tranzacții bancare și istoricul acestora, numerele cardurilor de plată, data expirării cardurilor, rechizitele remitenței de bani;
- 4.5.4. *date tehnice la utilizarea aplicației “MAIBank”*: OTP, adresa IP, sistemul și platforma de operare, tipul și marca dispozitivului mobil, date de localizare;
- 4.5.5. *adresa de domiciliu*;
- 4.5.6. *situația economico-financiară*.

**4.6. Sursele de proveniență** a datelor cu caracter personal, prelucrate în cadrul sistemului “MAIBank”, sunt următoarele:

- 4.6.1. cererea de deschidere a contului bancar persoanei fizice, la încheierea cu Banca a contractului de cont curent bancar pentru persoane fizice;
- 4.6.2. cererea de emitere card pentru persoane fizice, la încheierea cu Banca a contractului privind emiterea și utilizarea cardurilor de către persoanele fizice;
- 4.6.3. informațiile obținute nemijlocit prin intermediul aplicației mobile “MAIBank”.

**4.7. Termenul de prelucrare a datelor** este stabilit, astfel încât să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate. Banca este obligată legal să păstreze datele de identitate și înregistrările tuturor operațiunilor financiare, ce decurg din derularea relațiilor contractuale sau tranzacțiilor ocazionale, pe o perioadă de maxim 10 ani de la închiderea relației contractuale, respectiv de la realizarea tranzacției ocazionale, într-o formă corespunzătoare (5 ani pe suport de hârtie și, ulterior, până la 5 ani – în format electronic). La expirarea termenului de stocare, datele sunt distruse/șterse. În cazul obligațiilor expres prevăzute de lege, aceste date pot rămâne la păstrare ca document de arhivă.

**[Public]**

**4.8. Transmiterea datelor cu caracter personal în adresa unor persoane terțe** se efectuează numai în cazurile când acest fapt este în mod expres permis sau prescris de legislația în vigoare. Datele prelucrate în cadrul sistemului “MAIBank” pot fi transmise către terțe părți, și anume:

- 4.8.1. partenerilor contractuali ai Băncii, în volumul și limitele necesare realizării scopurilor pentru care datele respective sunt prelucrate;
- 4.8.2. autorităților de supraveghere, fiscale și/sau instanțe judecătorești sau altor organe abilitate prin lege, în cazurile când Banca este obligată să furnizeze astfel de informații în conformitate cu legislația în vigoare.

**4.9.** Datele prelucrate în cadrul sistemului “MAIBank” se transmit pentru executarea tranzacțiilor, companiei de procesare a tranzacțiilor cu cardurile de plată, care are calitatea de persoană împuternicită a operatorului.

**4.10.** Subiecții datelor cu caracter personal, prelucrate în cadrul sistemului “MAIBank”, **beneficiază de următoarele drepturi:**

- 4.10.1. să dispună de acces liber la datele sale cu caracter personal, inclusiv de dreptul de a efectua copiile datelor respective, cu excepția situațiilor prevăzute în legislația în vigoare;
- 4.10.2. dreptul de intervenție asupra datelor cu caracter personal, ce prevede rectificarea, actualizarea, blocarea sau ștergerea datelor cu caracter personal a căror prelucrare contravine legii, în special datorită caracterului incomplet sau inexact al datelor;
- 4.10.3. de a se opune în orice moment, în mod gratuit, din motive întemeiate și legitime legate de situația sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care legea stabilește altfel;
- 4.10.4. alte drepturi menționate în legislația Republicii Moldova, precum și în reglementările internaționale aplicabile.

**4.11.** Pentru a exercita unul sau mai multe drepturi privind prelucrarea datelor cu caracter personal în cadrul sistemului “MAIBank”, persoana vizată poate adresa o sesizare (cerere/reclamație) scrisă, datată și semnată, la sediul Băncii din mun. Chișinău, str. Constantin Tănase, nr. 9/1, sau prin e-mail: [protectiadatelor@maib.md](mailto:protectiadatelor@maib.md). Orice sesizare, adresată Băncii în scris, va fi procesată în modul corespunzător, conform ordinii stabilite în Bancă.

## **5. Securitatea Sistemului**

**5.1.** Securitatea Sistemului este asigurată prin următoarele cerințe de autentificare:

- 5.1.1. persoana poate să se conecteze la Sistem în calitate de Client doar în urma procedurii de activare a Profilului utilizatorului, descrisă în prezentele Condiții;
- 5.1.2. persoana poate să obțină acces la Sistem în baza autentificării prin PIN5 sau în baza autentificării biometrice încorporată în dispozitiv și OTP;
- 5.1.3. în cadrul sesiunii de utilizare a Sistemului, unele servicii care implică mișcări de fonduri în/din conturile Clientului sunt accesibile doar în baza autorizării suplimentare;
- 5.1.4. toate datele de comunicare în cadrul Sistemului sunt transmise în formă criptată.

**5.2.** Utilizatorul este responsabil pentru necompromiterea modurilor de autentificare, utilizate de el.

**5.3.** În scopul prevenirii compromiterii modurilor de autentificare Utilizatorul este obligat:

- 5.3.1. să nu înscrie pe vre-un suport care permite asocierea cu Sistemul, PIN5 sau parola de deblocare a dispozitivului mobil în cazul folosirii acesteia la accesarea Sistemului;
- 5.3.2. să modifice regulat parola de acces dedicată Sistemului, sau parola de deblocare a dispozitivului mobil în cazul folosirii acesteia la accesarea Sistemului;

**[Public]**

5.3.3. să asigure protejarea dispozitivului său mobil (smartphone, tabletă) utilizând softul specializat (antivirus, firewall etc.), politicile de limitare a accesului la resurse și alte metode de securitate a informației;

5.3.4. să limiteze accesul persoanelor terțe la dispozitivul /dispozitivele sale mobile (smartphone, tabletă);

5.3.5. să modifice imediat parola setată în cazul în care ea este compromisă;

5.3.6. să contacteze imediat Serviciul Contact Center al Băncii, în cazurile în care Utilizatorul nu are posibilitate de a efectua acțiunile menționate mai sus;

5.3.7. să anunțe imediat Banca și să comunice detaliile privind circumstanțele compromiterii informațiilor din Sistem și eventualele efecte ale acesteia.

**5.4. În cazul în care factorul de autentificare de tip OTP este compromis, Utilizatorul trebuie:**

5.4.1. să solicite operatorului de telefonie mobilă suspendarea numărului de telefon (utilizat în calitate de număr de telefon pentru parola OTP) și restabilirea accesului exclusiv al Utilizatorului la acest număr de telefon;

5.4.2. să solicite Băncii, prin contactarea Serviciului Contact Center al Băncii, blocarea temporară a Sistemului;

5.4.3. să solicite Băncii modificarea numărului de telefon utilizat în calitate de număr de telefon pentru OTP prin depunerea cererii corespunzătoare la Bancă.

**5.5. Banca recomandă următoarele modalități de utilizare securizată a aplicației “MAIBank” :**

5.5.1. să nu divulge informația confidențială altor persoane (PIN5, numărul de card, parole, conturi, datele personale);

5.5.2. să nu lase dispozitivul / dispozitivul “touch id / FingerPrint” fără supraveghere în special după procedura de autentificare și să asigure că ecranul dispozitivului nu este vizibil altor persoane;

5.5.3. să seteze parola de acces la dispozitivul mobil și opțiunea de blocare a dispozitivului după o perioadă de inactivitate;

5.5.4. să utilizeze parole și coduri de acces puternice, pentru a evita spargerea lor;

5.5.5. să utilizeze diferite parole pentru fiecare serviciu (poșta electronică, conturile de acces la rețelele de socializare, etc.);

5.5.6. să descarce aplicațiile mobile numai din magazinele oficiale AppStore și Google Play. Toate alte surse nu sunt oficiale și Banca nu poartă răspundere pentru consecințele instalării aplicațiilor descărcate din aceste surse;

5.5.7. să efectueze regulat actualizarea sistemului de operare, a aplicației “MAIBank” și ale altor aplicații instalate pe dispozitivul mobil, utilizând numai surse oficiale;

5.5.8. pentru a fi siguri că nu descărcați ceva dubios, dezactivați în setările telefonului pe platforma Android opțiunea „Surse Necunoscute” în setările de „Securitate”;

5.5.9. să instaleze pe dispozitivul mobil aplicații anti-virus și să le actualizeze regulat. De asemenea trebuie actualizată aplicația anti-virus la calculatoarele la care se conectează dispozitivul mobil;

5.5.10. să nu păstreze pe dispozitivul mobil informație confidențială (PIN coduri, numărul de card, parole de acces), de exemplu în mesaje SMS, E-mail-uri, mementouri, notițe, etc.;

5.5.11. sistemul “MAIBank” să fie utilizat numai de către Utilizatorul autentificat;

5.5.12. să șteargă informația confidențială în cazul transmiterii dispozitivului altor persoane (vinderea, reparația). Pentru aceasta este necesar să restabilească setările prestabilite

**[Public]**

din fabrică. Ștergerea informației cu utilizarea punctelor de meniu va permite infractorului restabilirea ei;

- 5.5.13. să activeze opțiunea de control la distanță pentru ștergerea datelor la distanță sau blocare în cazul pierderii dispozitivului;
- 5.5.14. să nu execute operațiunea de obținere a dreptului de administrator (jail-break, rooting). Aceste operațiuni pot scădea nivelul de securitate și expune Sistemul unor riscuri suplimentare;
- 5.5.15. în cazul pierderii sau furtului dispozitivului mobil, să informeze imediat Banca pentru blocarea Sistemului și a accesului la Sistem, să sune operatorul telefoniei mobile pentru blocarea cartei SIM;
- 5.5.16. în cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decât valabilitatea cartei SIM, să informeze Banca, pentru deconectarea Sistemului de la numărul de telefon pentru a evita compromiterea modalității de autentificare de tip OTP;
- 5.5.17. să fie vigilenți la atacurile de tip phishing scopul cărora este obținerea de la Utilizator a informației confidențiale. Să nu execute mesajele primite prin email sau SMS prin care se solicită divulgarea datelor confidențiale. Banca niciodată nu transmite mesaje SMS și email-uri pentru a solicita de la clienți informație confidențială;
- 5.5.18. să monitorizeze regulat operațiunile executate. Extrasul de cont și card primit de la Sistem, va permite depistarea la timp și semnalarea operativă a Băncii despre neregulile identificate;
- 5.5.19. în cazul nefuncționării cartei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este urmare a acțiunilor frauduloase;
- 5.5.20. să termine lucrul cu aplicația mobilă prin accesarea butonului Exit (Ieșire);
- 5.5.21. să ignore propunerile de instalare a unor aplicații sau update-uri dacă ele sunt primite de la persoane sau companii necunoscute, recepționate prin diferite modalități, de exemplu prin email-uri, SMS ș.a.
- 5.5.22. să evite utilizarea rețelelor wireless/Wi-Fi publice (ex. în magazin, aeroport, pe strada, în cafenea, etc.) pentru operațiuni bancare. Se recomandă să fie dezactivată opțiunea de conectare automată la Wi-Fi.

## **6. Drepturile și obligațiile Părților**

**6.1.** Părțile își asumă drepturile și obligațiile menționate expres în capitolul curent, în alte capitole ale prezentelor Condiții și alte documente transmise de către o Parte celeilalte Părți în legătură cu obiectul prezentelor Condiții.

### **6.2. Banca este obligată:**

- 6.2.1. să execute Tranzacțiile în conformitate cu regimul de prestare a Serviciului respectiv definit în prezentele Condiții;
- 6.2.2. să ia toate măsurile necesare pentru prevenirea riscurilor ce pot apărea în urma utilizării frauduloase a Sistemului și să asigure măsurile aplicate în vederea identificării Utilizatorului și asigurării confidențialității, autenticității și non-repudierii Tranzacțiilor;
- 6.2.3. să asigure un grad adecvat de securitate și siguranță operațională a localului, echipamentului de comunicații și procesare, precum și a soluției soft prin intermediul căreia se inițiază, înregistrează, controlează și recepționează Tranzacțiile;



**[Public]**

- 6.2.4. să asigure confidențialitatea datelor referitoare la Utilizator, precum și a Tranzacțiilor efectuate de acesta prin intermediul Sistemului, în conformitate cu prevederile legislației în vigoare aferente secretului comercial;
- 6.2.5. să asigure Utilizatorului posibilitatea de a anunța situațiile de urgență și să ia toate măsurile necesare pentru a stopa imediat executarea Tranzacțiilor frauduloase prin intermediul Sistemului din momentul în care a fost înștiințată, asigurând Utilizatorului mijloace care să poată dovedi că comunicarea a fost efectuată (data, ora înregistrării și numărul de înregistrare a comunicării);
- 6.2.6. să asigure identificarea și înscrierea corectă a acțiunilor Utilizatorului în Sistem, în baza actului de identitate al acestuia și/sau în baza altor documente și măsuri care permit identificarea Utilizatorului în conformitate cu actele normative în vigoare și riscurile potențiale;
- 6.2.7. să asigure stocarea și păstrarea informațiilor referitoare la Tranzacțiile efectuate prin intermediul Sistemului pentru perioadele de timp prevăzute de actele normative în vigoare, precum și să monitorizeze corespunderea Tranzacțiilor efectuate prin intermediul Sistemului condițiilor contractuale și normelor în vigoare;
- 6.2.8. să furnizeze Utilizatorului, periodic sau la cererea expresă a acestuia, informații referitoare la Tranzacțiile efectuate prin intermediul Sistemului sau informații privind situația contului bancar al Utilizatorului, în cazul în care acesta este Client. Aceste informații vor fi prezentate în conformitate cu prevederile contractuale existente dintre Bancă și Utilizator, cu respectarea prevederilor legislației în vigoare;
- 6.2.9. să crediteze contul bancar al Utilizatorului cu valoarea despăgubirilor din momentul recunoașterii dreptului Utilizatorului la acestea sau de la stabilirea acestui drept de către o instanță de judecată ori de arbitraj;
- 6.2.10. să asigure securitatea Sistemului “MAIBank”, cu condiția respectării de către Utilizator a măsurilor de securitate recomandate în prezentele Condiții.

**6.3. Utilizatorul este obligat:**

- 6.3.1. să ia cunoștință de prezentele Condiții înaintea logării în Sistem și să utilizeze Sistemul în strictă conformitate cu prevederile acestora;
- 6.3.2. să acceseze Sistemul prin intermediul telefonului mobil/ dispozitivului mobil în corespundere cu cerințele și ținând cont de recomandările indicate în prezentele Condiții;
- 6.3.3. în cazul autentificării prin utilizarea amprentei digitale, să activeze funcționalitatea de autentificare prin amprenta digitală pe dispozitivul “touch id / FingerPrint” și să înregistreze cel puțin una din amprentele personale pentru a controla accesul la dispozitivul “touch id / FingerPrint”, să selecteze autentificarea în Sistem prin amprenta digitală stocată în memoria dispozitivului “touch id / FingerPrint”;
- 6.3.4. să asigure confidențialitatea elementelor de autentificare (toate tipurile de parole), să ia măsuri rezonabile de protejare a acestora contra compromiterii și să nu admită utilizarea acestora de către terțe persoane;
- 6.3.5. să înștiințeze Banca (prin intermediul Serviciului Contact Cetner al Băncii sau la ghișeele Băncii) imediat ce constată:
  - a) modificarea neautorizată a soldului contului bancar;
  - b) orice eroare sau neregulă apărută în urma gestionării de către Bancă a contului bancar;
  - c) elementele ce creează suspiciuni cu privire la posibilitatea cunoașterii de către persoane neautorizate a factorilor de autentificare deținute de Utilizator;
  - d) dereglări ale Sistemului sau dacă parolele primite sunt incorecte;

**[Public]**

6.3.6. să manifeste o atitudine responsabilă privind asigurarea siguranței și securității sistemului.

**6.4. Banca are dreptul:**

6.4.1 să perceapă taxe și comisioane conform tarifelor în vigoare;

6.4.2 să nu primească spre executare prin intermediul Sistemului tranzacții care nu corepund prezentelor Condiții;

**6.5.** Banca nu poartă răspundere pentru cauzele de dispută ce ar putea interveni între Utilizator și beneficiarul plății ca urmare a modificării de către furnizor a structurii documentelor utilizate în cadrul plății, precum și a cauzelor în care cardul este blocat, expirat, are activat fereastra tranzacțională.

**6.6.** Banca nu poartă răspundere pentru daunele suportate de către Utilizator ca urmare a nerespectării recomandărilor de utilizare securizată a Sistemului, prevăzute în prezentele Condiții.

**7. Responsabilitatea Părților și ordinea repartizării pierderilor**

**7.1.** Utilizatorul este responsabil de veridicitatea și corectitudinea informației transmise prin intermediul Sistemului, pentru Tranzacțiile efectuate și documentele electronice transmise în adresa Băncii în cadrul sesiunii de utilizare a Sistemului.

**7.2.** Utilizatorul este responsabil de neadmiterea compromiterii modalităților de autentificare deținute.

**7.3.** Utilizatorul este responsabil de asigurarea acțiunii de **Log out / Ieșire** după fiecare sesiune de utilizare a Sistemului și să verifice corectitudinea documentelor electronice pregătite pentru a fi transmise spre executare, cât și a documentelor deja executate de către Bancă.

**7.4.** Banca și Utilizatorul recunosc puterea juridică a Tranzacțiilor efectuate în cadrul sesiunii de utilizare a sistemului „MAIBank”.

**7.5.** Banca și Utilizatorul recunosc, că documentele electronice transmise de către Utilizator Băncii și confirmate prin OTP sunt echivalente celor depuse personal de către Utilizator și semnate cu semnătura olografă a acestuia și produc aceleași drepturi și obligațiuni ale părților.

**7.6.** Banca va lua toate măsurile necesare pentru prevenirea riscurilor ce pot apărea din utilizarea frauduloasă a sistemului „MAIBank”.

**7.7.** Banca este responsabilă pentru neexecutarea sau executarea necorespunzătoare a Tranzacțiilor efectuate prin intermediul Sistemului:

7.7.1. în cazul în care executarea necorespunzătoare este atribuită unei disfuncționalități a Sistemului sau a unei componente a acestuia, cu condiția că dereglarea nu a fost cauzată intenționat de către Client;

7.7.2. chiar dacă Tranzacțiile au fost inițiate prin utilizarea mijloacelor care nu se află sub controlul Băncii, cu condiția să se facă dovada că Tranzacțiile a fost inițiate în conformitate cu prevederile prezentelor Condiții.

7.7.3. pentru Tranzacțiile inițiate după momentul notificării Băncii de către Utilizator a pierderii controlului asupra Sistemului (de exemplu funcționării defectuoase a Sistemului, compromiterea parolelor sau a altor informații sensibile de către persoane neautorizate etc.);

7.7.4. pentru pierderile suportate de către Utilizator ca rezultat al unei fraude comise de către o persoană sau grup de persoane terțe prin exploatarea unei vulnerabilități a Sistemului, cu condiția că Utilizatorul a respectat toate prevederile prezentelor Condiții.

**[Public]**

## **8. Dispozițiile finale**

**8.1.** Relațiile dintre Bancă și Utilizator care apar în rezultatul utilizării Sistemului „MAIBank” și care nu sunt specificate în prezentele Condiții, vor fi reglementate în conformitate cu Regulile de utilizare a cardului și/sau legislația în vigoare a Republicii Moldova.

**8.2.** Toate neînțelegerile și/sau litigiile apărute între Utilizator și Bancă pe marginea utilizării Sistemului „MAIBank” vor fi soluționate pe cale amiabilă, prin negociere. În cazul epuizării tuturor mijloacelor de soluționare pe cale amiabilă a litigiilor, acestea vor fi soluționate de către instanțele de judecată competente, în conformitate cu legislația Republicii Moldova.

**8.3.** Banca va informa Utilizatorii privind modificarea prezentelor Condiții și/sau tarifelor aferente serviciilor integrate în Sistem prin afișarea versiunii(lor) modificate a(ale) acestor documente pe pagina Web a Băncii ([www.maib.md](http://www.maib.md)) cu cel puțin 2 luni până la data intrării în vigoare a acestora.