

TERMS AND CONDITIONS OF USE OF THE MYIUTE REMOTE-ACCESS INFORMATION SYSTEM

I. THE MYIUTE REMOTE-ACCESS INFORMATION SYSTEM AND ACCEPTANCE OF USE OF THE SYSTEM:

1. MyIute remote-access information system is made available by O.C.N. “IuteCredit” LLC (hereinafter referred to as “**IuteCredit**” or the “**Company**”), with its registered office in Chişinău municipality, 182 Ştefan cel Mare şi Sfânt Blvd., 5th floor.

2. The terms and conditions for the use of the MyIute remote-access information system (hereinafter referred to as the “**MyIute Terms**”), as set out in this document, are and shall be governed by and construed in accordance with the law of the Republic of Moldova. **By accessing, using or registering to benefit from the MyIute System, you accept and agree to be bound by these MyIute Terms.**

3. These MyIute Terms constitute the legal agreement between the Company and the User governing access Customer to and use of the **MyIute System**. Creating a MyIute profile, submitting a product application, completing customer onboarding and establishing a contractual relationship are separate stages. Creation of a profile or storage of a draft application does not, by itself, mean that customer due diligence has been completed, that a business relationship has been established, or that the Company has approved or granted any product.

4. We recommend that you read these MyIute Terms in full before deciding whether to accept them and whether you wish to continue the registration and/or login process in the System. If you do not agree with any of the provisions of these MyIute Terms, or if you refuse to have your personal data processed as notified to you through the Personal Data Processing Policy of O.C.N. “IuteCredit” LLC on the Company’s website: <https://iute.md/politica-de-confidentialitate/>, please do not access, browse or use the application, nor the services, information, materials and other content contained therein.

5. Upon the first successful login to the System, in order to use its functionalities, the User shall review the MyIute Terms and accept them.

6. Acceptance of the MyIute Terms takes place by pressing the “Continue” button, whereby you express your consent to the use of the MyIute System under the conditions set out in the MyIute Terms and in the Personal Data Processing Policy of O.C.N. “IuteCredit” LLC. The Company reserves the right, at any time, at its sole discretion, to modify and/or discontinue, temporarily or permanently, the MyIute System (or part of its functionalities), with or without notice to the Customer. The Company shall not be liable to the Customer and/or third parties for any modification, suspension or discontinuation of the service provided through the application. Where the Customer fails to comply with the MyIute Terms, access to the service within the System may be suspended and/or blocked by the Company without notice to the Customer and without payment of any compensation to the Customer.

7. In order to use the System, you must be at least 18 years of age and have full legal capacity to give your consent to these Terms.

iute Moldova

 Chişinău,
Ştefan cel Mare şi Sfânt, 182

 iute.md
022 801 500



8. By pressing the “Continue” button, you declare and warrant the following:

- that you have the right, authority and full legal capacity to access and use the application;
- that you agree to the MyIute Terms and understand that you are bound by them;
- that you have been informed of the personal data processing conditions set out in the Personal Data Processing Policy of O.C.N. “IuteCredit” LLC published on the Company’s website, and that you agree to it;
- that, by using the MyIute System, you will not breach any law or regulation of the Republic of Moldova, and that you are solely responsible for compliance with all applicable local laws and regulations.

9. Where campaigns and promotions are carried out, their special terms and conditions may apply. Such terms and conditions may be presented in brief form within the System, on a merchant’s website, or at a place of business of the Company or of the merchant.

10. A person who is at least 18 years old and holds a valid Moldovan personal identification number (IDNP) may initiate profile creation in the MyIute mobile application. The profile is created only after successful electronic identity verification. To establish a business relationship, sign an agreement or obtain access to regulated products or services, the applicant must successfully complete the applicable onboarding requirements, including electronic identity verification, customer due diligence, AML/CFT screening and customer risk classification. The Company may refuse, suspend, restrict or escalate the process where verification fails, information is incomplete, screening or risk results require review, or applicable law or internal AML/CFT rules so require.

11. The MyIute Terms are legally binding and take effect from the moment of accessing the System, and both parties undertake to comply with them when using and providing IuteCredit services through the MyIute System.

II. DEFINITIONS:

a) **Customer or User** – a natural person who is in the process of establishing, or has already established, a business relationship with the Company, , or/and who has downloaded, installed, accessed and/or uses the MyIute System.

b) **Personal data** – any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified.

c) **MyIute System** – a secure remote-access information system, accessible through a device running the iOS or Android operating system, connected to the internet, available on Google Play and the App Store. The device used must be compatible with the System. The System is intended exclusively for private and personal use. Through the MyIute System, the Company’s Customers can access their credit account online, carry out certain transactions and/or contract for certain services remotely, via the internet, without the need to be physically present at a subdivision of the Company. Access to, and the availability of, the functionalities

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



may vary depending on the type of services offered and the Company's policy at any given time. Certain functionalities may also be made available through a web interface; access to that interface is confirmed through the MyIute mobile application registered on the Customer's device. The MyIute System is also used by applicants who have not yet established a business relationship with the Company, for the purpose of creating a profile and of completing the onboarding process.

d) **Passcode** – a confidential numeric code chosen by the Customer and used as part of the device-bound strong customer authentication mechanism for login, approval and agreement signing. A cryptographic key pair is generated in the secure hardware of the registered device; the private key remains on that device and is protected by the passcode. Where enabled, device biometrics may be used to unlock the credential. The passcode must not be disclosed to any third party. Customer Customer The passcode consists of six digits and is set and confirmed by the Customer in the mobile application. The certificate associated with the key pair is issued by the Company's certification service and is revoked when the passcode is reset or when the registered device is changed.

e) **“Digital Onboarding” remote identification IT solution** – the set of technological elements used within the MyIute mobile application to carry out the electronic identification process for natural persons who are citizens of the Republic of Moldova, holders of a personal identification number (IDNP), at least 18 years of age, for the purpose of onboarding (initiating a business relationship with the Company/updating its data) and benefiting from the specific products and services offered by the Company. This solution enables the transmission, processing and automatic validation of identification data, images of the identity document and of the User's face captured live within the application, and information communicated by the User, for the purpose of verifying his/her identity without physical presence. The process also involves verifying the data provided against the information available in the State Population Register and in other official sources, in accordance with the legal requirements on the prevention of money laundering, combating the financing of terrorism, identification of politically exposed persons and verification of the information declared in respect of tax residence, as well as with Regulation No. 281/2024 of the National Bank of Moldova on the requirements for the identification and verification of the identity of customers by electronic means. The solution does not permit the use of photographs or video recordings made previously; the images of the identity document and of the User's face are captured live, within the application, and are subject to movement/liveness detection checks.

f) **MyIute Terms** – The terms and conditions for use of the MyIute System set out in this document constitute the legal contract concluded between the Company and the Customer. The MyIute Terms establish the manner in which Customers may be onboarded (initiate a business relationship with the Company), update their data, and use the MyIute System in order to benefit from the specific products and services offered by the Company.

III. LOGIN TO MYIUTE:

12. CustomerAccess to the MyIute System is initiated by entering the personal identification number (IDNP). For this purpose, the Customer shall hold a mobile telephone number declared to the Company, connected to one of the mobile telephony operators of the Republic of Moldova and capable of receiving SMS messages, as well as, where strong customer authentication has been set up, the mobile device registered in the MyIute System.

13. To use the MyIute System, you must be a natural person, at least 18 years of age, holding a valid identity document and a personal identification number (IDNP) issued in the Republic of Moldova. The MyIute System may be used exclusively to carry out transactions in one's own name.

14. In order for the Company to fulfil its obligations arising from Law No. 308 of 22.12.2017 on the prevention and combating of money laundering and terrorist financing, from Regulation No. 281/2024 of the National Bank of Moldova on the requirements for the identification and verification of the identity of customers by electronic means, and from Law No. 195/2024 on the protection of personal data, the Company shall process personal data for the purpose of identifying the Customer and authenticating him/her within the MyIute System, ensuring the security of transactions, and applying precautionary measures for the prevention of online identity theft.

15. The System may only be used if the device used to access it is secured by a password, fingerprint, Face ID or another security method offered by the device.

16. The purpose of the MyIute System is to implement a secure method of identifying Customers within the system, thereby guaranteeing Users a higher level of security, facilitating remote access for Customers to the System, and enabling the Customer to carry out frequent operations remotely, securely and without physical presence.

17. Registration of the User shall be carried out by the Company applying its Customer authentication (login) procedure. Registration involves the processing of certain personal data, as notified to you through the Personal Data Processing Policy of O.C.N. "IuteCredit" LLC on the Company's website. After logging in to the System, the User is requested to create a six-digit passcode and, optionally, to enable biometric unlocking; through these actions, the User also sets the strong customer authentication, i.e. establishes the mechanism by which the Company securely validates his/her identity. The setting of the passcode is preceded by electronic identity verification. When the passcode is set, a cryptographic key pair is generated in the secure hardware of the device: the private key remains on the device, protected by the passcode, and never leaves it, while the corresponding certificate is issued by the Company's certification service and registered for that device. Biometric unlocking, where enabled by the User, only unlocks the key protected by the passcode and does not replace the passcode.

18. Access to MyIute is linked to the registered User and, for device-bound strong customer authentication, to one registered mobile device at a time. A registered device may not be used as the active MyIute device for multiple Users, and a User may not use MyIute simultaneously on multiple active devices. When changing devices or resetting a passcode, the Company may require phone-number verification and renewed electronic identity verification, revoke the previous credential, deactivate the former device registration and issue a new device-bound credential. Before a change of device is carried out, the User is warned that the registration on the previous device will be

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



deactivated and shall confirm the change.

18A. Mobile login may require the User to unlock the device-bound private key using the passcode or an enabled biometric method and to sign a one-time challenge. Web access, where made available, may require approval through the registered MyIute mobile application, including number matching, passcode or biometric confirmation and a time-limited device-signed response. Failed, expired, cancelled or mismatched challenges may be rejected and may trigger lockout or other security controls. Where a passcode has not yet been set, access through the web interface cannot be completed; the User is directed to the mobile application, by means of a QR code or of a download link, in order to carry out identity verification and set the passcode. The Company applies validity periods, limits on the number of attempts and temporary blocking in respect of one-time passwords, of confirmation requests and of the entry of the passcode.

18B. Where the User resets a forgotten passcode or changes the registered device, the following steps are applied: verification of the possession of the declared telephone number by means of a one-time password; renewed electronic identity verification, by means of the identity document and biometric verification; deactivation of the registration of the previous device, where applicable; setting of a new passcode;. Where identity verification is not successful, the reset is refused and access to the MyIute System is not granted.

18C. Agreements, applications and other documents made available in the MyIute System are signed by the User by entering the one-time authentication code sent via SMS,. By accepting the MyIute Terms, the User agrees that the application of the authentication code sent via sms in this manner constitutes the User's electronic signature, that it produces the legal effects agreed between the parties and that the Company is entitled to rely on it as proof of the User's consent. Documents may be signed in the MyIute System only in one's own name.

19. The User's data, including the data provided in the "Know Your Customer" form, must be true and up to date in order to access the System.

20. In order to use the System, the User must allow it access to certain functions of the device necessary for the proper operation of the MyIute System. Use of the System is equivalent to the User's consent to the MyIute System's access to the device's functions. Such functions include, in particular, access to the camera, for the purpose of capturing the identity document and the facial image, access to the secure hardware of the device, for the purpose of generating and storing the authentication credentials, for the purpose of confirming logins and operations. In accordance with the applicable regulatory requirements, the Company also collects and retains the technical data of the device used, including the model and parameters of the device, the version of the application and of the operating system, the IP address and the network connection data, the time zone and the language settings, for the purposes of identification, of the prevention of fraud and of the security of the process.

21. The Customer agrees and understands that he/she is responsible for maintaining the confidentiality of the login data associated with the use of the System and for taking reasonable measures to keep such information confidential.

22. User profiles are not transferable to any other third party.

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



23. The User must ensure that the information included in the profile is up to date, complete, accurate and reliable.

24. The Customer undertakes to notify the Company immediately, without undue delay, upon becoming aware of the loss, theft, unlawful appropriation or unauthorised use of his/her login data, as well as of the mobile phone used to access the application. You also agree to notify the Company immediately, without undue delay, in the same manner, of any other security breach related to the services provided through the System of which you become aware.

IV. GENERAL CONDITIONS FOR THE USE OF THE “DIGITAL ONBOARDING” REMOTE IDENTIFICATION IT SOLUTION:

25. Digital onboarding is a remote process conducted through the MyIute mobile application. It may include: collection and verification of the User’s IDNP, phone number and e-mail address; verification of the phone number by a six-digit one-time password sent by SMS and valid for a limited period; electronic identity verification through an integrated third-party e-KYC solution, including capture and verification of the identity document and biometric/liveness checks; setup of device-bound strong customer authentication; collection or confirmation of official and residential address information, nationality, place of birth, tax residence and citizenship; completion of the applicable customer due diligence questionnaire; review and confirmation of the collected data; AML/CFT screening and risk classification; and, where required, manual review by the Company. Customer

- **Profile and application status.** A customer record or draft product application may be stored during onboarding, but no application processing or credit decisioning occurs until the onboarding requirements have been successfully completed.
- **CDD questionnaire.** The User is asked to provide information including PEP or PEP-associate status, the purpose of the business relationship, source of income, employment status and employment sector. The questionnaire and answer options may vary according to country, customer risk level and the active version configured by the Company.
- **Screening and risk assessment.** The Company assesses the User on a risk-sensitive basis using customer data, questionnaire answers, sanctions, PEP and adverse-media screening, and other permitted information. Lower-risk outcomes may be approved automatically; higher-risk, unacceptable or otherwise flagged outcomes may be referred for manual review, remain pending, be rejected, or result in permanent blocking where appropriate.
- **Verification of the telephone number.** The telephone number declared by the User is verified by means of a six-digit one-time password (OTP) transmitted by SMS, valid for three minutes. Where the code is not entered within that period, it is invalidated and the User shall request the transmission of a new code or restart the process. The remote procedure may be completed only where the one-time password has been transmitted and validated. The Customer’s record is created in the Company’s systems only after the telephone number has been successfully verified.



- **Electronic identity verification.** Verification is carried out through the e-KYC solution integrated in the mobile application, operated by a specialised provider engaged by the Company. It involves the prior consent of the User, the granting of access to the camera, the live capture of both sides of the identity document and of the facial image, movement/liveness detection checks, the automatic verification of the authenticity and validity of the document, the comparison of the facial image with the photograph in the document and the cross-checking of the data with the State Population Register. The result is transmitted to the Company in a digitally signed form and is verified by the Company before being recorded.

- **Address and personal information.** The data relating to the official address is pre-filled on the basis of the response received from the state register, and the User confirms or completes it and may declare a different residential address. The User also provides information concerning nationality, place of birth, tax residence and citizenship.

- **Review of the data.** Before the data is submitted for assessment, the User is presented with all the data collected in the course of onboarding and may either confirm it or return in order to correct it.

- **Agreement signing and access to the product.** Where an agreement is concluded, it is signed by one-time authentication code sent via SMS, and access to the product or service is granted only after the User has been successfully onboarded and the agreement has been signed.

26. In order to guarantee the safety and transparency of our services, the Company applies strict identification procedures for all persons initiating a business relationship with the Company through electronic channels, in full compliance with the legislation of the Republic of Moldova on the prevention and combating of money laundering and terrorist financing (AML/CFT) and with Regulation No. 281/2024 of the National Bank of Moldova on the requirements for the identification and verification of the identity of customers by electronic means.

26A. Before accessing the remote identification solution, the Company makes available to the User these MyIute Terms, the information note concerning the processing and protection of personal data, and a summary version of its policy on the prevention of money laundering and terrorist financing, which describes the identification of the Customer, the customer due diligence measures applied and the treatment of politically exposed persons. The electronic identification process is preceded by the User's consent to the processing of personal data, including biometric data.

27. Each applicant undergoes an electronic identification process, within which the following measures are applied:

- verification of the validity and authenticity of the identity document;
- collection, where applicable, of other relevant information, depending on legal requirements and the Customer's risk profile;
- automatic assessment of the information provided by the User for the purpose of establishing his/her true identity;

iute Moldova



Chişinău,
Ştefan cel Mare şi Sfânt, 182



iute.md
022 801 500



- verification of the telephone number and of the electronic mail address by means of a one-time password, without the validation of which the process cannot be completed;
- live capture of the identity document, on both sides, and of the facial image, together with movement/liveness detection checks; the loading of photographs or video recordings made previously is not permitted;
- automatic verification of the security elements, of the design and of the machine-readable zone of the document, and comparison of the facial image with the photograph in the identity document;
- cross-checking of the data declared with the data available in the State Population Register;
- verification of the applicant against the international and European Union sanctions lists, against the lists relating to terrorism and to the proliferation of weapons, in respect of the status of politically exposed person and against information from credible public sources;
- recording and retention of the technical data of the device used and of the images and information captured in the course of the process;
- The data provided is processed under conditions of maximum security and is used exclusively for the purpose of identifying and verifying the Customer, assessing the risk associated with the Customer and complying with legal obligations.

27A. The Company does not initiate the business relationship by electronic means where the standard customer due diligence measures cannot be applied, where the technical requirements of the identification solution are not met, or where the identity of the applicant cannot be verified. In such cases the electronic identification is recorded as unsuccessful, the onboarding process is not completed, and the applicant may be invited to initiate the business relationship in the presence of a representative of the Company.

27B. Where there are suspicions as to the existence of a defect of consent, including physical or psychological pressure exercised upon the applicant, or other suspicions concerning the identification process, the Company shall request the applicant's physical presence at one of its subdivisions. Where there are doubts as to the veracity of the data or of the documents presented, the Company may request additional information or confirmations, or the application of an electronic signature to a copy of the identity document.

28. The Company strictly complies with AML/CFT rules, including:

- identification and monitoring of politically exposed persons (PEPs), their family members and persons known to be close associates thereof;
- applying precautionary measures depending on the type of business relationship and the transactions carried out.

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



- CustomerWhere the applicant declares, or where screening indicates, that the applicant is a politically exposed person, a family member of such a person or a person known to be a close associate thereof, enhanced customer due diligence measures are applied and the file is submitted for manual review and for the decision of the Company's authorised risk and compliance function. The Company may also require the business relationship to be initiated by physical presence at one of its subdivisions, on the basis of an individual assessment.

29. The information provided by the Customer is collected and stored in secure information systems, accessible only to authorised personnel and used exclusively for purposes permitted by law. The Company will not disclose the information to third parties except in situations expressly provided for by the applicable legal framework or on a justified legal basis. The documents and information obtained in the course of electronic identification, including the images captured, the copies of the identity documents, the technical data of the device used and the IP address, are retained for the entire period of the business relationship and for five years following its termination, and are made available, upon request, to the National Bank of Moldova, to the Office for Prevention and Fight against Money Laundering and to the law enforcement authorities.

30. The Customer is obliged to provide correct, complete and true information at all stages of the identification process, and to update his/her personal data at the Company's request or whenever changes occur. By accepting the MyIute Terms, you confirm that all information provided is true and that the funds used in the relationship with the Company originate from legal sources.

30A. Following the completion of the customer due diligence questionnaire, the Company determines the Customer's risk level automatically, by means of an internal decision engine, on the basis of weighted criteria configured in its AML/CFT settings. The criteria include, in particular, the tax residence, the official address, the place of birth, the citizenship and the age of the Customer, the onboarding method used, the answers given in the questionnaire (the status of politically exposed person or of a person associated with such a person, the source of income, the purpose of the business relationship, the employment status and the employment sector), as well as the results of the screening carried out against sanctions lists, lists of politically exposed persons and adverse media sources. The Customer is classified in one of the following risk levels: low, low to medium, medium, medium to high, high or unacceptable.

31. The Company applies ongoing customer due diligence on a risk-sensitive basis throughout the customer lifecycle, irrespective of whether the Customer has an outstanding loan. Upon login and on the occurrence of relevant events, the Company may verify whether identity verification has been completed, whether the Customer has a valid CDD questionnaire, whether the applicable renewal date has passed or is approaching, and whether other triggers require updated information, including expiry of identification data, changes in risk profile, a new product application, or indicators of suspicious or unusual activity.Customer

31A. If a CDD questionnaire or required customer-data update has expired, the Customer must complete or confirm the requested information before continuing to use the MyIute application, and



access may be restricted until completion. Where renewal is approaching, the Company may offer the Customer an early, optional update. The timing and content of renewal requests may vary according to the Customer's current risk classification, regulatory requirements and the Company's AML/CFT settings. Where the Customer has not previously completed electronic identity verification, the questionnaire is not requested until that verification has been completed. Where the questionnaire expires within the following 30 days, its completion is offered as an optional step, which the Customer may postpone. The period of validity of the questionnaire is established for each risk level in the Company's AML/CFT settings, and the period preceding expiry may be amended by the Company.

31B. Screening and risk information may be received asynchronously from specialist service providers. If later results indicate a higher risk level or otherwise require action, the Company may update the Customer's classification, create a compliance review, request additional information, restrict access or services, reject the risk, or take other measures permitted by law and internal AML/CFT rules. The Company also carries out the ongoing monitoring of the business relationship and of transactions, including by automated means, for the purpose of identifying unusual or suspicious operations. Where suspicions of money laundering or of terrorist financing are identified, the Company shall inform the Office for Prevention and Fight against Money Laundering, in accordance with the law, and is not entitled to inform the Customer thereof.

31C. Customers identified and onboarded by the Company before the entry into force of the customer due diligence process described in this Section shall be requested to complete the customer due diligence questionnaire upon their first subsequent login to the MyIute application.

32. The Company reserves the right to restrict access to Digital Onboarding for natural persons from certain jurisdictions considered high-risk from an AML/CFT regulatory perspective or subject to international sanctions.

33. The Company does not establish business relationships with persons or entities involved in the financing of terrorism, listed under international sanctions, or presenting an unacceptable level of risk from an AML/CFT regulatory perspective.

34. The Company may refuse to initiate, or may terminate, the contractual relationship at any time in the event of reasonable suspicions regarding the legality of the funds, the purpose of the relationship or the accuracy of the information provided, as well as for other reasons justified under its internal policies.

34A. The Company records the stage reached by each applicant or Customer in the onboarding process by means of an onboarding status. Only a Customer holding the status of fully onboarded customer may conclude an agreement with the Company and benefit from the products and services made available in the MyIute System. The following statuses may be applied: (i) onboarded — all the data and checks required under the applicable rules are available and the Customer may enter into a contractual relationship with the Company; (ii) initially onboarded — a prospective Customer who does not hold all the data required in order to enter into a contractual relationship; (iii) verification failed — the electronic identity verification was not successful; (iv) onboarding pending — the file is pending the completion of customer due diligence activities, such as the review of an AML/CFT

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



check or of the risk assessment; (v) risk not accepted — the risk associated with the Customer has not been accepted, this status being capable of amendment only manually and following a new assessment; and (vi) blacklisted — the Customer is permanently excluded, for example where the Customer is subject to international sanctions or where fraud has been established.

35. The Company may also use the “Digital Onboarding” remote identification IT solution for updating Customers’ data.

35A. For the purpose of carrying out the onboarding process and the ongoing customer due diligence, the Company uses specialised service providers, in particular for electronic identity verification, for screening and monitoring for AML/CFT purposes, for the transmission of SMS messages, for the issuing of certificates and for the hosting of the information systems. Those providers act on the basis of a contract concluded with the Company and in accordance with its instructions, and the Company remains responsible for compliance with the requirements applicable to the identification and verification of the identity of Customers by electronic means.

V. FUNCTIONALITIES OF THE MYIUTE SYSTEM:

36. The MyIute System offers, without limitation, the following functionalities:

- digital onboarding of the Customer through the “Digital Onboarding” remote identification IT solution;
- updating of the Customer’s data through the “Digital Onboarding” remote identification IT solution;
- receiving real-time notifications from the Company regarding various financial transactions and activities, as well as account updates;
- installation of the application through Google Play/App Store;
- submitting a loan application, which may be stored in draft form during onboarding; requests to income and credit registries, application assessment and credit decisioning are initiated only after the User has been successfully onboarded;
- purchasing an insurance policy;
- disconnecting/blocking the Company’s Customer from MyIute where the Customer breaches the rules for carrying out operations through MyIute;
- the possibility of learning about the Company’s current offers.
- completion of the customer due diligence questionnaire and updating of the Customer’s data;
- setting, changing and resetting the passcode, and managing the registered device;
- signing agreements and other documents by means of the one-time authentication code sent via SMS;



- confirming logins carried out through the web interface, where that interface is made available.

37. The Company shall periodically review its offering of digital functionalities. The functionalities available as of this date may be supplemented with new ones and will be communicated in the MyIute System User Manual. Some functionalities may be restricted from/excluded from the Company's digital offering, at any time, for any reason, with or without notice. Some functionalities are accessible only within the operating day.

41. The functionalities available through the System may offer the possibility of uploading, posting, downloading or transmitting content. In such case, the User is responsible for the content that he/she has uploaded, posted, downloaded or transmitted through the System.

42. The Company reserves the right to remove or to refuse to post content that violates the MyIute Terms or the applicable regulatory framework, but this does not mean that the Company continuously monitors, analyses or verifies any content.

VI. RIGHTS AND OBLIGATIONS OF THE PARTIES:

43. As an existing Customer of the Company, you have the following rights:

- to receive advice in the event of any uncertainties, by contacting Customer Support during the working hours established for business days;
- to change or reset the passcode and to enable or disable biometric unlocking, subject to the verification of the declared telephone number and to renewed electronic identity verification;
- at any time after accepting these MyIute Terms, to stop using the MyIute System.

44. At the same time, you are obliged to:

- not provide the Company with false, incorrect or outdated data that may mislead the Company's system;
- not enter personal data that is incorrect or does not belong to you. Fraudulent use of another person's personal data may give rise to administrative or criminal liability;
- maintain a method for unlocking the phone for as long as the MyIute System is installed on it;
- not access links, install applications, or respond to messages or calls requesting personal data or confidential information. Likewise, do not install remote-control applications or any other applications or updates from unknown sources, unofficial updates, or any software that could allow unauthorised access to your mobile device, credentials or accounts. Where these obligations are breached, or where a third party is, intentionally or through negligence, allowed access to the device, the authentication data, or the authorisation or security codes of the User, the User shall be deemed to have authorised that third party to act in his/her name and on his/her behalf. The User bears full responsibility for any transaction carried out through the System,

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



including transactions, payments, credits or other operations initiated by third parties through the use of disclosed or compromised data and access;

- not disclose the phone's unlock password/security code to any third party, since disclosing it exposes you to the risk of unauthorised access to your MyIute profile and of operations being carried out in your name. You are solely responsible for maintaining the confidentiality of, and safekeeping, the data entered into the MyIute System and the phone's unlock password/security code, the passcode and the OTP code. Furthermore, you are responsible for any activities of any nature that take place on the account;

- not allow the biometric data (fingerprints or Face ID) of other persons to be registered on the phone where you activate biometric data for authentication in the MyIute System, given that, in such case, access to the System and the authorisation of transactions could be carried out using any of the biometric data added to the phone;

- notify us immediately of any unauthorised use of the System installed on your personal phone number, or of any breach of the security of the phone and/or of the login data for the System of which you become aware, or which you ought reasonably to suspect;

- not disclose to third parties the OTP code received on your personal phone number, or the passcode or any other code used to authenticate, or to sign documents in MyIute, since their disclosure allows operations to be authorised in your name;

- notify us of the loss, theft, or unauthorised access to, the mobile phone on which the MyIute System is installed, immediately upon becoming aware of such a situation. Should you fail to fulfil the above-mentioned obligation, you assume full liability for all operations that unauthorised persons might carry out through the MyIute System, or as a result of identification carried out through the System installed on the phone number declared to the Company during a call to/from the Company's Contact Centre or at a Company unit, including access to any information or the updating of data;

- uninstall the System where the phone on which you initially installed it no longer belongs to you, or where you will no longer use it;

- not falsify or provide erroneous information regarding your identity or intentions, or anything related to the System;

- not transmit, distribute or offer any information or materials that are wholly or partly unlawful, false, fraudulent or inappropriate, offensive, or that violate public order and morality;

- confirm or update your identification data, the validity of your identity documents, and other information whenever necessary, as requested by the Company;

- ensure and maintain the physical and logical security of the phone, in accordance with the manufacturer's recommendations and good practice;

- update the phone's operating system in accordance with the manufacturer's recommendations, and use only official versions of the operating system provided by the manufacturer;
- not bypass the security protections of the operating systems recommended by the mobile phone manufacturer;
- install the MyIute System only from the official sources of the dedicated stores – Google Play Market or App Store – published at the Company's request;
- ensure that data is entered into the System correctly and completely;
- not infringe any right provided by law, any property right, any intangible right, the right to privacy, or the like;
- not use the content of the System to resell, distribute or otherwise use the services offered for any purpose other than that permitted under these MyIute Terms;
- not distribute the offers contained in the MyIute System;
- not misuse and/or use in bad faith and/or for fraudulent purposes the functionalities offered within the System, and not attempt to access them by any method other than through the interface and instructions made available by the Company;
- not upload, access, post, e-mail, or otherwise transmit, any material containing viruses or other computer code, files or programs intended to interrupt, destroy or limit the functionality of the System or of any other electronic service or functionality available within the System.

45. The Company reserves the right:

- to temporarily suspend or to cancel the Customer's account in the event of the User's breach of the provisions of these MyIute Terms or other actions that do not fall within applicable rules and policies;
- to process personal data in accordance with the Personal Data Processing Policy of O.C.N. "IuteCredit" LLC on the Company's website: <https://iute.md/politica-de-confidentialitate/>;
- to verify and modify/update Customers' data in order to comply with legal requirements applicable to the Company's activity;
- to implement changes, improvements, security updates and bug fixes, in order to optimise the user experience and ensure the proper functioning of the System;
- to amend the MyIute Terms, the updated version of which will be published in the System and on the Company's website. It is the User's responsibility to read the MyIute Terms and the Personal Data Processing Policy of O.C.N. "IuteCredit" LLC on the Company's



website before using the System. Continued use of the System after the posting of any amendment or supplement shall constitute the User's acceptance thereof;

- to update, improve or otherwise modify the System at any time, for any reason, with or without notice. These MyIute Terms shall apply to all such updates, improvements or modifications of the System;
- to suspend use of the System during maintenance periods (whether scheduled or unscheduled) or in the event of technical malfunctions or other circumstances. In such case, the operations requested by the Customer may be carried out through physical presence at the Company, in accordance with the conditions and fees established by the Company for such operations.

46. The Company undertakes:

- to ensure the protection and confidentiality of personal data;
- to maintain the confidentiality of information concerning the transactions/payment operations and accounts of the Customer managed by the Company through the MyIute System;
- to properly inform the Customer and to provide support in the use of the MyIute System;
- to register/modify Customers' data in accordance with the requirements of the Company's internal regulations;
- to receive, register and process Customers' requests and applications during the working hours established for business days;
- to block the Customer's access to the System at his/her request, received by telephone or e-mail on business days and in accordance with the Company's working schedule;
- to offer Customers the possibility of withdrawing their consent to the processing of personal data in accordance with the legal conditions;
- to maintain the optimal level of security and to implement all measures necessary to protect Users' personal and financial data;
- to execute, on behalf of the Customer, the transactions authorised by the Customer, in accordance with the operating-day schedule for the provision of the relevant service, as defined in the MyIute Terms.

VII. PROCESSING OF PERSONAL DATA:

47. The Company, as a personal data controller, processes the personal data of Customers wishing to use the MyIute System in accordance with the applicable legal provisions in the field of personal data protection and as set out in the Personal Data Processing Policy of O.C.N. "IuteCredit" LLC, available at: <https://iute.md/politica-de-confidentialitate/>.

48. In order to provide the functionalities of the MyIute System, the Company uses the service

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



providers referred to in clause 35A. Those providers process personal data on the basis of a contract concluded with the Company and solely in accordance with its instructions, save where they act as independent controllers, in which case the processing is also subject to the conditions of their own privacy policies.

48A. In the course of the onboarding process and of the ongoing customer due diligence, the Company carries out automated processing, including profiling, for the purposes of verifying identity, determining the risk level, screening the Customer and, where a product application is submitted, assessing creditworthiness. Such processing is necessary for the conclusion and performance of the agreement and for compliance with the Company's legal obligations, whereas the processing of biometric data is carried out on the basis of the Customer's explicit consent, given before the identification process begins. Where a decision is taken exclusively by automated means and produces legal effects in respect of the Customer, the Customer has the right to obtain human intervention on the part of the Company, to express his/her point of view and to contest the decision, by writing to the address dpo@iute.md.

49. The data subject has the following rights: the right of access, the right to be informed, the right to rectification, the right to erasure, the right to restriction of processing, the right to object, the right to data portability, the right to withdraw consent at any time, without affecting the lawfulness of the processing carried out before the withdrawal, the right not to be subject to a decision based exclusively on automated processing, and the right to lodge a complaint with the National Centre for Personal Data Protection. The data subject may exercise these rights by writing to the following e-mail address: dpo@iute.md. Requests are answered within one month of receipt, a period which may be extended by two months where the complexity or the number of requests so requires.

VIII. INTELLECTUAL PROPERTY RIGHTS:

50. The entire content of the MyIute System – images, texts, graphics, symbols, graphic elements, scripts, programs and other data – is the property of the Company and its suppliers and is protected by copyright law and by the laws on intellectual and industrial property. Use, without the Company's consent, of any of the elements listed above shall be sanctioned in accordance with applicable legislation.

IX. JUSTIFICATION ON ACCOUNT OF AN IMPEDIMENT:

51. The Company shall not be liable to the User for the non-fulfilment of any obligations justified by an impediment/force majeure event beyond its control, nor for the operation and connection of other national or foreign networks, or for their activities and actions in general. An impediment beyond its control/case of force majeure may include, for example but without limitation: a state of war (whether declared or not), armed conflict, revolution, insurrection, military or terrorist actions or threats, sabotage, civil unrest, strikes or other industrial action, laws, regulations, decisions or directives, natural disasters, earthquake, fire, explosion, solar or meteorological disturbances, public emergencies, or any other occurrence that is beyond its control. The Company will take all measures necessary to ensure the maximum availability of the application in the event of impediments

iute Moldova



Chişinău,
Stefan cel Mare şi Sfânt, 182



iute.md
022 801 500



beyond its control and in cases of force majeure, i.e. events that are beyond its control.

X. TERMINATION OF USE OF MYIUTE:

52. Termination of the User's use of the MyIute System may occur in the following situations:

- a)** at the User's initiative, by uninstalling the System from his/her device or by requesting the blocking of access; uninstalling the application does not terminate the business relationship, the agreements concluded or the obligations arising from them;
- b)** at the Company's initiative, in the event of the User's breach of the provisions of these MyIute Terms;
- c)** Customer where the business relationship between the Customer and the Company ends;
- d)** where the Customer is assigned the status of risk not accepted or of blacklisted Customer, in accordance with clause 34A.

XI. WHAT WE ARE NOT RESPONSIBLE FOR:

53. We provide the MyIute System for personal use only. Not all MyIute System services will function on all mobile equipment.

54. You accept that the System will not be delivered free of errors or on an uninterrupted basis, and that certain imperfections will not be corrected at the time they occur.

XII. FINAL PROVISIONS:

55. The Company may suspend or modify the MyIute System immediately, for any reason, including where repair or maintenance work is required. We may periodically add new features and are under no obligation to provide any particular feature through MyIute. We may withdraw MyIute, but in such case we will notify you at least 30 days in advance.

56. Where additional services are implemented and made available within the MyIute System, such services shall be subject to the same rules and conditions contained in these clauses, unless they are subject to separate conditions.

57. Any disagreements and/or disputes arising between the Customer and the Company on the basis of the use of the MyIute System shall be settled amicably, through negotiation between the parties. Where all means of amicable settlement of disputes have been exhausted, they shall be settled by the competent courts, in accordance with the legislation of the Republic of Moldova.

XIII. CONTACT INFORMATION:

58. If you have any questions or uncertainties regarding the MyIute Terms, please contact us at:

- **E-mail:** info@iute.md;
- **Telephone:** +373 22 801 500;
- **Address:** mun. Chişinău, 182 Ştefan cel Mare şi Sfânt Blvd., 5th floor, Republic of Moldova.

iute Moldova



Chişinău,
Ştefan cel Mare şi Sfânt, 182



iute.md
022 801 500

