



የኢትዮጵያ ብሔራዊ ባንክ  
**NATIONAL BANK OF ETHIOPIA**  
አዲስ አበባ / ADDIS ABABA

**Requirements for Information Technology (IT) Management  
of Microfinance Institution Directive No. MFI/33/2022**

**Whereas**, a business process supported by information technology improves the efficiency, effectiveness and competitiveness of a microfinance institution;

**Whereas**, some microfinance institutions are running their operations manually or their operations are inadequately supported with information technology;

**Whereas**, it has become important to require microfinance institutions to automate at least their core business processes and their management information system;

**Whereas**, risks related to the usage of information technology should be adequately and periodically identified and managed to ensure the safety and soundness of individual microfinance institution and the microfinance sector as a whole;

**Now, therefore**, in accordance with Articles 14(2) (e) and article 34(2) of the Microfinance Business Proclamation No. 626/2009 (as amended by Proclamation No.1164/2019), the National Bank of Ethiopia has issued this Directive.

**1. Short Title**

This Directive may be cited as “**Requirements for Information Technology (IT) Management of Microfinance Institution Directive No. MFI/33/2022**”

**2. Definitions**

For the purpose of this Directive, unless the context provides otherwise:

- 2.1 “**Automate**” means fully supporting and enabling a business process with information technology;
- 2.2 “**Core business process**” means customer due diligence, loan processing, loan disbursement & collection, loan portfolio management, deposit collection and withdrawal, accounting, and local money transfer service;
- 2.3 “**Cyber security**” means preservation of confidentiality, integrity and availability of information systems and ensuring the resilience of a microfinance institution to a cyber-attack;



- 2.4 **“Disaster recovery site”** means a place where a microfinance institution places its backup facility that enables to recovery and restore its IT system and operation when a primary datacenter become unavailable;
- 2.5 **“Information technology (IT)”** means an integrated set of computer hardware, software, networks and processes that collects, stores, processes and transmits data to provide information and helps to carry out operations and facilitate interaction with internal and external customers/stakeholders of a microfinance institution;
- 2.6 **“Information technology incident”** means an event that jeopardizes the information system processes, storages or transmissions and disrupts operation process of a microfinance institution;
- 2.7 **“Information technology risks”** means potential events that result in failure of IT and disrupting business of a microfinance institution;
- 2.8 **“INSA”** means Information Network Security Agency;
- 2.9 **“IT vendor”** means a person or an organization that offers IT goods or services to a microfinance institution for sale;
- 2.10 **“Management information system”** means an automated system consisting of computer hardware & software, processes, people and procedures that gathers data from multiple systems; analyzes the data and generates information or reports that help board and senior management of a microfinance institution and the National Bank in their decision making, oversight, and risk management roles;
- 2.11 **“Microfinance institution”** means a company licensed by the National Bank to engage in microfinance business;
- 2.12 **“National Bank”** means National Bank of Ethiopia;
- 2.13 **“Senior management”** means chief executive officer, senior executive officer, and any other officers as defined by each microfinance institution, responsible for running day-to-day activities of the institution;
- 2.14 **“Third party service provider”** means a person or an entity to whom the microfinance institution outsourced some of its activities and/or who gets access to confidential information through its provision of services to the institution.

### 3. Scope of the Directive

This Directive shall apply to all microfinance institutions operating in Ethiopia.

### 4. General Requirements

- 4.1. A microfinance institution shall describe and include the role of IT in its business strategy.
- 4.2. A microfinance institution shall develop and implement IT strategy.
- 4.3. IT strategy referred to in sub-article 4.2 hereinabove shall be aligned with the institution’s business strategy and shall cover at a minimum:
- i) the institution’s vision, mission, and strategic objectives;



*[Handwritten signature]*



- ii) assessment of information technology opportunities, threats and internal strengths and weaknesses to manage information technologies;
  - iii) assessment of stock of existing IT and planned ones to be introduced in the future;
  - iv) IT objectives to be pursued;
  - v) key performance indicators in achieving IT objectives;
  - vi) strategies to ensure security in the usage of IT;
  - vii) identified IT initiatives to achieve indicated objectives; and
  - viii) requirements provided by Information Network Security Agency (INSA) or any other competent authority.
- 4.4. To ensure proper implementation of the IT strategy indicated under 4.2 and 4.3 of this Article, a microfinance institution shall develop and implement:
- i) IT governance, including duties and responsibilities of board, senior management, IT department, risk management and internal audit functions and other relevant organs of the institution;
  - ii) IT department structure with its duties and responsibilities;
  - iii) IT policies and procedures; and
  - iv) annual IT plans with allocation of duties and responsibilities among all responsible organs of the institution.
- 4.5. A microfinance institution shall allocate financial and human resources that would enable it to effectively and efficiently implement its IT strategy and IT risk management program.
- 4.6. To ensure proper implementation of IT related initiatives and projects, a microfinance institution shall develop and follow effective project and IT vendor management framework.
- 4.7. Board and senior management of a microfinance institution shall at least quarterly review progress in implementation of IT related plans and initiative or projects and shall take corrective measure (if required).

## **5. Requirements for Automation of Core Business Processes**

- 5.1. A microfinance institution shall fully automate at a minimum its core business processes so as to improve the efficiency and effectiveness of its operations, customer service delivery and risk management, among others.
- 5.2. The automated core business of a microfinance institution shall be interoperable with one another to ensure automated data sharing and communication among the IT systems.
- 5.3. A microfinance institution shall fully automate and put in place a robust, secure, efficient and comprehensive management information system commensurate with the scale and complexity of the institution's operations that at a minimum supports:



*[Handwritten signature]*

- i) generation of periodic operational and financial performance reports of the various businesses of the institution;
- ii) senior management in its decision making and risk management process;
- iii) board of directors and its sub-committees in their oversight functions;
- iv) proper exercise of shareholders right including getting the necessary and relevant information; and
- v) generation of periodic supervisory returns or reports as required by the National Bank.

5.4. The automation of core business processes and management information system, as indicated under sub-article 5.1, 5.2 and 5.3 of this Article, shall ensure timely delivery of services and submission of supervisory returns.

## **6. Management of IT Risks**

6.1. A microfinance institution shall put in place and implement IT risk management program aligned with the institutions' risk management program.

6.2. The IT risk management program indicated under sub-article 6.1 of this Article shall at least cover:

- i. types or categories and definitions of IT risks to which the institution is exposed;
- ii. IT risk management culture and objectives;
- iii. IT risk identification, assessment, measurement, reporting and monitoring mechanisms;
- iv. duties and responsibilities of board and/or its committees, senior management and/or its committees, risk management function, and operational units in managing the risk;
- v. IT risk management policies, procedures, and standards; and
- vi. duties and responsibilities of internal auditor to assess and assure the adequacy of IT risk management processes and the overall program.

6.3. In the course of automating its various businesses and developing program to manage related risks, a microfinance institution shall take into account cyber security risk management requirements provided by INSA.

6.4. A microfinance institution shall conduct quarterly IT risk assessment and present the assessment report to the board of directors for its discussion and direction.

6.5. The IT risk assessment report indicated under sub-article 6.4 hereinabove shall be submitted to the Microfinance Institutions Supervision Directorate of the National Bank within 30 (thirty) calendar days after end of each quarter.

6.6. A microfinance institution shall maintain and quarterly update IT risk register which facilitates the monitoring and managing of the risks.



*Handwritten signature in blue ink.*



6.7. A microfinance institution shall set up or build a disaster recovery site that is maintained at safe place with adequate detachment from the main site of the IT systems.

## **7. IT Risks Management Policies**

7.1. A microfinance institution shall develop and implement IT risk management strategies, plans, policies, procedures and standards so as to achieve its risk management objectives.

7.2. The IT risk management strategies, plans, policies, procedures and standards indicated under sub-article 7.1 hereinabove shall at least cover:

- i) physical access and network securities;
- ii) business continuity plan;
- iii) disaster recovery plan;
- iv) incident response plan;
- v) hardware, software and network maintenance;
- vi) database and backup management and access;
- vii) IT change and patch management system;
- viii) IT vendor and third party service provider management;
- ix) customer data privacy;
- x) password, data transfer security, user right access, antivirus, and firewall security; and
- xi) managing risk related to system development, integration and acquisition.

7.3. A microfinance institution shall periodically revise its IT risk management strategies, plans, policies, procedures and standards based on its periodic IT risk assessment findings.

## **8. Training and Awareness**

8.1. A microfinance institution shall prepare annual IT security awareness plan to enhance awareness of all concerned stakeholders regarding IT strategy, policies, procedures, and IT risk management of the institution.

8.2. The awareness program indicated under sub-article 8.1 hereinabove shall be provided to all relevant employees of the institution having stake in the implementation of IT strategy and managing of related risks, including board and senior management of the institution.

8.3. Based on training need assessment, a microfinance institution shall develop and implement annual training plan to train all the staffs of IT department of the institution on an ongoing and regular basis.



*[Handwritten signature]*

## 9. IT Audit

- 9.1. A microfinance institution shall establish an IT audit function within its internal audit function.
- 9.2. The IT audit function shall be allocated with human and financial resources which are commensurate with the size and complexity of the microfinance institution.
- 9.3. The IT audit function shall prepare and implement annual audit plan that gives assurance on the effectiveness of IT strategy, policies, procedures, plans, governance, and risk management.
- 9.4. The scope of the IT audit shall at least include:
  - i. evaluating and determining the effectiveness of IT strategy, plans, governance, initiatives, policies & procedures and practices;
  - ii. determining proper implementation of IT strategy, governance, plans, initiatives and compliances with policies and procedures;
  - iii. evaluating the adequacy of IT risk management process and practices;
  - iv. carrying out at least annual cyber threat test or conducting other IT audit activities as provided by INSA or other competent authority; and
  - v. identifying areas of deficiencies, recommending corrective actions and following up the rectification of audit findings to ensure that the senior management effectively implements the required actions.
- 9.5. IT audit shall be conducted at least on a quarterly basis, and the findings shall be reported to board audit committee of the institution and a copy shall be submitted to Microfinance Institutions Supervision Directorate of the National Bank.
- 9.6. A microfinance institution shall make all necessary arrangements for its IT audit staffs for their attainment of information security audit certification from any concerned local Government organ.

## 10. Reporting

- 10.1. A microfinance institution shall notify Microfinance Institutions Supervision Directorate of the National Bank within **2 (two) working** days any IT incidents that could have significant impact on the institution's ability to provide services to its customers and/or adversely affect the institution's reputation or financial condition as per the format attached to this Directive (**Annex-1**).
- 10.2. A microfinance institution shall quarterly submit to Microfinance Institutions Supervision Directorate of the National Bank concerning its ongoing handling of IT incidents as per the format attached to this Directive (**Annex-2**).



*[Handwritten signature]*



## **11. Transitional Provisions**

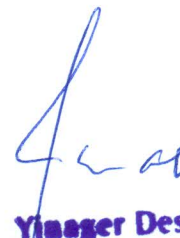
- 11.1. A microfinance institution shall implement all the requirements of Article 5 and sub-article 6.7 of this Directive within **3 (three) years** starting from the effective date of this Directive.
- 11.2. All provisions of this Directive except Article 5 and sub-article 6.7 shall be effective after the elapse of **1 (one) year** starting from the effective date of this Directive.

## **12. Penalty**

- 12.1. A microfinance institution that violates sub-article 11.1 of this Directive, or fails to fully automate any of its core businesses and its management information system as set out under Article 5 and set up its disaster recovery site as per sub-article of 6.7 of this Directive within:
- i) the given period shall be penalized Birr 10,000 per each requirement on monthly basis up until it fully complies with the requirement; and
  - ii) additional **2 (two) years** may result in full or partial suspension of related core business in due consideration of the nature of the function.
- 12.2. A microfinance institution that violates other provisions of this Directive shall be penalized as per relevant National Bank directive.

## **13. Effective Date**

This Directive shall enter into force as of the **1<sup>st</sup> day of April 2022**.

  
**Yineger Dessie (PhD)**  
**Governor**



**Annex-1:**

Name of the Microfinance Institution: \_\_\_\_\_

Reporting Period: \_\_\_\_\_

**High Impact IT Incident Report**

No.	Data and time of the incident	Description of the incident, its nature, sources ...	Impact of the incident

Prepared by: \_\_\_\_\_ Approved by \_\_\_\_\_

Signature: \_\_\_\_\_ Signature: \_\_\_\_\_

**Annex-2**

Name of the Microfinance Institution: \_\_\_\_\_

Reporting Period: \_\_\_\_\_

**Quarterly IT Incident Report**

No.	Data and time of the incident	Description of the incident, its nature, sources ...	Impact of the incident	Action taken so far to resolve it	Current status of the incident (resolved or not)	Action taken to mitigate future similar incidents

Prepared by: \_\_\_\_\_ Approved by \_\_\_\_\_

Signature: \_\_\_\_\_ Signature: \_\_\_\_\_



*Handwritten signature in blue ink.*