ESAF FINANCIAL HOLDINGS

INFORMATION TECHNOLOGY/ SYSTEM POLICY

Approver	Board of Directors
Approved on	08.04.2023
Policy Owner	Secretariat of the Company
Review frequency	Annual
Version	V1

Document History :

Revision No.	Revision Date	Amendment Description
1.	05.07.2024	Annual Review
2.	27.06.2025	Annual Review

CONTENTS

1. Introduction 3
2. Objective of the Policy 3
3. Policy Background 4
4. Board Oversight 4
5. Security Aspects 4
6. Information Security and Cyber Security 6
7. Business Continuity Planning (BCP) 9
8. Back-up of Data with Periodic Testing 9

1. Introduction

The Information Technology / System Policy provides for an integrated set of protection measures that must be uniformly applied across ESAF Financial Holdings Private Ltd to ensure a safe and secured environment for its operations.

The information processing resources of the Company generate, store and retrieve information like customer information, organisational information, daily operations related information etc., which is supported by IT systems, Process and People that are important assets of ESAF Financial Holdings Private Ltd. Hence the Company needs to implement processes and controls to protect the confidentiality, integrity and the availability of such information to ensure that the information is available to authorised individuals only, when it is required.

Reserve Bank of India vide its circular RBI/DNBS/2016-17/53 (Master Direction DNBS. PPD.No.04/66.15.001/2016-17) of June 8, 2017 has given guidelines for Information Technology Framework for the NBFC sector. This IT Framework falls within the scope of Section B of the Guidelines i.e. NBFCs with asset size of below INR 500 crores (Indian Rupees Five Hundred Crores only).

Presently, the Company do not have any IT system since the operation of the Company is limited to the investment in the equity and Tier II bonds of the ESAF Small Finance Bank only and also the Company has not raised any public funds. There is no other customers for the Company and hence there is no customer interface required. Only a readymade single user accounting software is used to keep its books of accounts. Hence the policy set forth below may not be applicable fully at present. However, these need to be applied as and when the Company develops or uses separate IT systems.

2. Objective of the Policy

The Information Technology/System Policy addresses the information security requirements of maintaining:

Confidentiality: Assurance that information is accessible only to those authorized to have access.

Integrity: Assurance of the completeness and accuracy of information and its processing.

Availability: Assurance that authorized users have access to information and associated assets when required

3. Policy Background

IT governance is an integral part of corporate governance of ESAF Financial Holdings Private Ltd, and effective IT governance is the responsibility of the Board of Directors of ESAF Financial Holdings Private Ltd and its executive management.

ESAF Financial Holdings Private Ltd has designated CFO as the Chief Information Officer of its IT operations and the Board exercises oversight on the CFO. The CFO ensures implementation of this IT Framework which, inter alia, includes not limited to (i) Security aspects; (ii) User Role; (iii) Information Security and Cybersecurity; (iv) Business Continuity Planning Policy; (v) Back-up Data..

4. Board Oversight

The Board has overall charge of the operational functions of ESAF Financial Holdings Private Ltd. The Board is further responsible for timely amending this IT Framework pursuant to its operations and/or any change in the regulations or new regulations issued by the RBI in relation to this Information Technology / System Policy.

5. Security Aspects

(i) Acceptable IT Usage

It is imperative to ensure that all the users and staff at ESAF Financial Holdings Private Ltd are aware of their responsibilities towards the IT Resources of the Company. The following guidelines shall be adhered to:

- ESAF Financial Holdings Private Ltd's staffs have been provided with a company desktop / laptop or portable electronic device. It is the staffs' responsibility for the proper care and use of their desktop / laptop / Portable Electronic Device, data and accompanying software while using the same.
- All electronic communication should be courteous, professional and business like as they may be subject to discovery in both criminal and civil proceedings.
- Intellectual property guidelines are to be observed.

- Employees must not copy, modify or transmit documents, software, information or other materials protected by copyright, trademark, patent or trade secrecy laws without authorization of the owner of such rights in such materials.
- Accessing another individual's electronic mail and other electronic media should only be done where Employees have a legitimate business need and with the knowledge and approval of that individual or the responsible partner.

(ii) Password Policy

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. The following password policy to be followed

- A strong password must be at least 8 (Eight) characters long.
- It should not contain any of the user's personal information—specifically his/her real name, user name, or even company name.
- It must be very unique from the passwords used previously by the users.
- It should not contain any word spelled completely.
- It should contain characters from the four primary categories i.e. uppercase letters lowercase letters, numbers, and special characters.
- To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 90 (Ninety) days.
- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.
- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be force changed immediately by the user to ensure confidentiality of all information.
- Under no circumstances, the users shall use another user's account or password that is sharing of password must not be there.

(iii) Access Controls

- Access to the ESAF Financial Holdings Private Ltd's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by

law and ESAF Financial Holdings Private Ltd's policies including but not limited to requirements laid down in this policy.

- Persons or entities with access to the ESAF Financial Holdings Private Ltd's electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by ESAF Financial Holdings Private Ltd, irrespective of the medium on which the information resides.
- Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person.

- Requirements:

  a. All users must use a unique ID to access ESAF Financial Holdings Private Ltd systems and applications.
  b. Remote access to ESAF Financial Holdings Services Ltd systems and applications must use a two-factor authentication
  c. System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

6. Information Security and Cyber Security

(i) Information Security

ESAF Financial Holdings Private Ltd has an information security framework with the following principles

- **Identification and classification of information assets:** ESAF Financial Holdings Private Ltd maintains detailed inventory of information asset with distinct and clear identification of the asset.
- **Role based access control** – Access to information is based on well-defined user roles (system administrator, user manager, application owner.). ESAF Financial Holdings Private Ltd has a clear delegation of authority to upgrade/change user profiles and permissions and also key business parameters
- **Personnel Security** - A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose potential threat to systems and data. ESAF Financial Holdings Private Ltd has a process of appropriate checks and balances to avoid any such threat to its systems and data.

- **Physical Security -** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. ESAF Financial Holdings Private Ltd has created a secured environment for physical security of information assets such as secure location of critical data
- **Environmental Security -** Environmental security measures must be adopted to reduce exposure to environmental threats arising due to events such as air conditioning failure, water seepage, cyclones, floods and earthquakes. Adequate controls shall also be in place to address the threats due to power failures and fire.
- **Network Security -** Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access. ESAF Financial Holdings Services Ltd's Network infrastructure shall be protected from unauthorised access by deploying required firewalls and other security measures.
- **Maker-checker –** Maker checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information. ESAF Financial Holdings Services Ltd ensures that it complies with this requirement to carry out all its business operations.
- **Digital Signatures -** A Digital signature certificate authenticates entity's identity electronically. ESAF Financial Holdings Private Ltd protects the authenticity and integrity of important electronic documents.
- **Regulatory Returns –** ESAF Financial Holdings Private Ltd has adequate system and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorized representatives of ESAF Financial Holdings Private Ltd.
- **Email Security –** The e-mail system of ESAF Financial Holdings Private Ltd shall be configured and managed to provide high availability, optimum performance and protection against various sources of threats such as malicious codes, unauthorised access, and data leakage. E-mail is a business communication tool and all users of ESAF Financial Holdings Private Ltd must use this tool in a responsible, effective and lawful manner. Email access from external network should be restricted by default to all the users.
- **Website & Application Security -** Proper procedures, access controls and security requirements in line with the standard industry practices shall be adhered to while maintaining software, applications and add-on modules from time to time. ESAF Financial Holdings Private Ltd shall ensure that the Website and all applications and

their respective CMS (Content Management System), 3rd party plugins, codes, etc., are updated to the latest versions. Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, should be installed on the machine.

- **Antivirus -** Malicious codes such as viruses, worms, Trojans, spy ware, root-kits etc. represent a significant threat to the performance and security of the ESAF Financial Holdings Private Ltd information processing resources and it can corrupt or destroy data or may spread confidential information to unauthorised recipients, resulting in loss of Confidentiality, Integrity and Availability of the information. ESAF Financial Holdings Private Ltd.'s Information Technology assets shall be protected against malicious code with anti-virus solution capable of early detection, efficient containment and eradication of malicious code. All servers, desktops and laptops shall be scanned for viruses and malwares on a periodic basis

(ii) Cyber Security

- ESAF Financial Holdings Private Ltd takes effective measures to prevent cyber-attacks and to promptly detect any cyber- intrusions to respond / recover / contain the fall out. Among other things, ESAF Financial Holdings Private Ltd takes necessary preventive and corrective measures in addressing various types of cyber threats which includes denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds and password related frauds.

- ESAF Financial Holdings Private Ltd realizes that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. ESAF Financial Holdings Private Ltd ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats.

(iii) Data Privacy

- ESAF Financial Holdings Private Ltd, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.

- Access to customer information by employees of the service provider to ESAF Financial Holdings Services Ltd is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the activity or outsourced function.

7. Business Continuity Planning (BCP)

- BCP forms a significant part of any organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP at ESAF Financial Holdings Private Ltd is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.

- The CFO is responsible for formulation, review and monitoring of BCP to ensure continued effectiveness including identifying critical business verticals, locations and shared resources to prepare a detailed business impact analysis.

8. Back-up of Data with Periodic Testing

- In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out.
- Restoration testing on a time to time basis is done as both hard disks and magnetic tapes are prone to errors.