EDC LIMITED

A Government of Goa Undertaking

INFORMATION SECURITY (IS) POLICY

SUMMARY OF POLICY:

Policy Name	INFORMATION SECURITY (IS) POLICY
Issue and Effective date	25.09.2025
Periodicity of Review	As decided by the Board of EDC
Owner/Contact	Computer Cell
Approver	Board of Directors (405th Board Meeting dated 25/09/2025)

INFORMATION SECURITY (IS) POLICY

1. Purpose

This policy outlines the framework and guiding principles adopted by EDC Ltd., a Non-Banking Financial Company (NBFC), for managing information security. It ensures the confidentiality, integrity, and availability of EDC's information assets, protects stakeholders' interests, and complies with regulatory requirements.

Existing Infrastructure and Backup Policy

Server Infrastructure:

- The Loan Manager web application is hosted on Amazon Web Services (AWS) cloud infrastructure.
- Users access the application through a web interface connected to the AWS-hosted environment.

Backup Frequency and Responsibility:

a) AWS Team

- A daily snapshot of the entire server is taken by the AWS team.
- This snapshot is scheduled every day at 11:30 PM (IST).

b) Computer Cell

- The Computer Cell has scheduled database backup on server every 2 hours.
- Complete database daily backup is stored and copied on OneDrive as well as on local portable storage devices.

c) End Users

- Users operate on laptops/desktops, maintaining their own data locally.
- OneDrive is used to synchronize user files and folders in real time, ensuring data is backed up continuously to the cloud.

2. Objectives

- To ensure protection of EDC's information systems and data against internal and external threats.
- To define responsibilities related to information.
- To ensure business continuity and minimize damage from security incidents.
- To comply with regulatory and legal obligations (RBI, IT Act, etc.).

3. Scope

This policy applies to:

- All employees of EDC Ltd.
- All information systems, infrastructure, networks, and applications owned or

operated by EDC.

- All information assets, whether digital or physical, processed or stored within EDC systems.

4. Information Security Objectives

- Protect customer and business data from unauthorized access and disclosure.
- Ensure ongoing regulatory compliance with RBI and IT Act.
- Establish a secure and resilient IT infrastructure.
- Promote a culture of user awareness and accountability throughout the organization.

5. Roles and Responsibilities

- Management: Oversight and approval of policy and security budgets.
- Computer Cell: Implement and monitor security controls, manage risks, and incident response.
- Employees: Follow information security guidelines and report violations or threats.

6. Information Security Measures

Access Control

- Access should be granted on a need-to-know basis.
- Use of unique credentials with Multi-Factor Authentication (MFA) should be kept mandatory.
- Access rights must be reviewed and updated periodically.

Asset Identification and Classification

- All information assets should be inventoried and classified based on criticality and sensitivity.
- Periodic asset reviews and ownership mapping should be done mandatory.

Role-Based Access Control (RBAC)

- Access should be granted strictly based on job roles and responsibilities.
- Computer Cell shall have a clear delegation of authority to upgrade RBAC/change user profiles and permissions.

Physical Security

- CCTV surveillance should be in place.

Network and System Security

- Regular security updates of systems must be checked.
- Unauthorized devices and software installations should be strictly prohibited.
- Systems should be deep scanned for any malware or virus at least once in a month.

Maker-Checker Mechanism

- There will be a maker-checker mechanism for all critical and financial transactions.
- Access to perform maker or checker roles should be controlled via role-based access control (RBAC) and reviewed periodically.

Audit Trails

- All system and user activities should be logged and monitored.
- Logs to be retained for at a minimum period of 2 years.

Email, One Drive and Internet Usage

- Official email accounts must be used for all work-related communication.
- Email systems should be protected with anti-spam, anti-phishing, and DLP mechanisms.
- Staff must keep their work data synced with OneDrive for secure and reliable access.

- Marketing Team should manage EDC's social media accounts using Multi-Factor-Authentication (MFA) and unique strong passwords for each of EDC's social media accounts.

7. Review and Updates

This policy will be reviewed annually or as and when there are changes in regulatory or operational requirements.

****