EDC LIMITED

A Government of Goa Undertaking

CYBER SECURITY POLICY

SUMMARY OF POLICY:

Policy Name	CYBER SECURITY POLICY
Issue and Effective date	30/03/2026
Periodicity of Review	As decided by the Board of EDC
Owner/Contact	Computer Cell
Approver	Board of Directors (407th Board Meeting dated 30/03/2026)

INDEX

Cyber Security Policy

1. Purpose

The purpose of this Cyber Security Policy is to establish a comprehensive framework for safeguarding the information systems, network infrastructure, and digital assets of EDC Limited against cyber threats and security incidents. The policy aims to ensure the confidentiality, integrity, and availability of information assets by implementing appropriate security controls, risk management practices, and governance mechanisms.

2. Objectives

- Protect EDC Limited's information assets from cyber threats.
- Ensure the confidentiality, integrity, and availability of financial and customer data.
- Secure all IT infrastructure including servers, desktops, laptops, and network devices.
- Establish preventive, detective, and corrective security controls.
- Ensure regulatory compliance and effective cyber risk management.
- Maintain business continuity in the event of cyber incidents.

3. Scope

This Cyber Security Policy applies to the following:

3.1 Personnel

- All employees
- Contract staff
- System administrators

3.2 IT Infrastructure

The policy covers all information systems used by EDC Limited including:

- Employee desktops, laptops and storage drives
- Application and database servers
- Mobile devices used for official purposes
- Network infrastructure including routers, switches, and firewalls

4. Cyber Threat Overview

EDC Limited recognizes the following major cyber threats:

4.1 Phishing Attacks

Phishing involves fraudulent emails or messages designed to deceive employees into revealing sensitive information such as login credentials or financial data.

Security Measures

- Email security shall be implemented using Microsoft 365 Exchange Online Protection (EOP) with anti-spam, anti-malware, and anti-phishing filtering enabled to detect and block malicious emails
- Multi-Factor Authentication (MFA) shall be enforced for all user accounts to prevent unauthorized access even if credentials are compromised
- Employees shall be made aware of the threats along with dos and don'ts periodically
- Suspicious email shall be reported to computer cell team for its review

4.2 Malware and Ransomware

Malicious software can infect systems, steal data, or disrupt operations. Ransomware may lock critical systems and demand payment to restore access.

Security Measures

- Endpoint protection software shall be deployed with real-time threat detection and centralized policy management to prevent and remediate malware infections
- Systems shall be regularly updated with security patches to address known vulnerabilities and reduce exposure to exploits
- Periodic system monitoring shall be implemented to detect abnormal behavior, unauthorized changes, or potential ransomware activity
- Regular data backups shall be maintained in secure and segregated locations with periodic restoration testing to ensure data recovery in case of incidents

4.3 Insider Threats

Users with authorized system access may intentionally or unintentionally compromise sensitive information.

Security Measures

- Role-based access control (RBAC) shall be enforced to restrict user access
- User access rights shall be reviewed periodically, including identification and removal of dormant, excess, or unauthorized privileges

- User activities on critical systems shall be logged and monitored to detect anomalous behavior, data misuse, or policy violations
- Segregation of duties shall be implemented through maker-checker controls to ensure critical transactions and system changes require dual authorization

4.4 Network Security Risks

Unsecured networks may expose systems to unauthorized access, data interception, or cyber-attacks such as intrusion and denial-of-service.

Security Measures

- Firewall protection shall be implemented on systems, periodic review, and logging to restrict unauthorized network traffic
- Critical systems shall be hosted within segregated network zones with appropriate access controls
- Secure communication protocols (such as HTTPS etc) shall be enforced to protect data

5. Information Asset Classification

Information assets shall be classified as follows:

Classification	Description
Confidential	Customer financial data and loan information
Restricted	System credentials and internal security data
Internal	Internal business information
Public	Information approved for public release

Appropriate security controls shall be applied based on the classification level.

6. Endpoint Security (User Desktops and Laptops)

User devices such as desktops and laptops represent a common entry point for cyber threats. EDC Limited shall implement the following Security Measures:

- Microsoft Defender Antivirus shall be deployed on all desktops/laptops with real-time protection, threat intelligence, automatic security updates, and centralized monitoring through Microsoft security console.
- Operating systems and critical applications shall be configured for automatic updates to ensure timely patching of security vulnerabilities
- Strong password policies shall be enforced, including complexity requirements, periodic changes, and account lockout after failed attempts

- Systems shall be configured with automatic screen lock / session log out after defined inactivity to prevent unauthorized access
- Restriction on installation of unauthorized software
- Use of external storage devices (e.g., USB drives) shall be blocked unless specifically needed

All laptops used for official work shall comply with organizational security standards.

7. Network Security and Wi-Fi Infrastructure

The organization's network infrastructure including routers, switches, and wireless networks shall be secured through the following measures:

- Routers and switches shall be securely configured by disabling unused ports/services, changing default credentials, and maintaining configuration backups
- Wi-Fi access shall be protected using strong authentication mechanisms (e.g., WPA2/WPA3-Enterprise with centralized user authentication)
- Internal and guest networks shall be logically segregated with restricted routing to prevent unauthorized access to critical systems.

8. Access Control and Authentication

Access to systems shall be governed by the principle of least privilege, ensuring users are granted only the access required for their job roles.

Security controls include:

- Unique user IDs shall be assigned to each employee to ensure accountability, traceability, and maintenance of audit trails
- Strong password policies shall be enforced, including complexity requirements, expiry controls, and account lockout after defined failed login attempts
- Multi-Factor Authentication (MFA) shall be enabled for critical systems and remote access to mitigate risks of credential compromise
- Role-based access controls (RBAC) shall be implemented with maker-checker principles, ensuring access is aligned to job responsibilities and approved through defined workflows
- User access rights shall be reviewed periodically, including privileged accounts, with audit trails maintained for all modifications.

Access rights shall be revoked immediately upon employee exit or role change, ensuring no residual or unauthorized access remains.

9. Data Protection and Backup

EDC Limited shall ensure protection of critical business data through the following controls:

- Regular backups of critical business and operational data shall be performed to ensure data recoverability in the event of system failure, cyber incidents, or other disruptions.
- Backup copies shall be stored securely, including offsite or alternate location storage where necessary, to ensure protection against data loss due to physical or system-related incidents.
- Access to backup data shall be restricted to authorized personnel only.

Periodic verification and testing of backup integrity shall be conducted to ensure that data can be successfully restored when required

10. Monitoring and Security Logging

System activities shall be continuously monitored to detect suspicious behavior, security incidents, and policy violations.

Monitoring mechanisms:

- Security logs shall be centrally collected and reviewed to identify anomalies, unauthorized activities, and potential security incidents
- Endpoint security alerts (e.g., Microsoft Defender) shall be actively monitored and investigated for malware, ransomware, or suspicious activities
- Unauthorized login attempts shall be tracked with alerting mechanisms and account lockout controls to prevent brute-force attacks

Security logs shall be retained for a period of 1 year.

11. Cyber Incident Response

EDC Limited shall maintain a structured and documented Cyber Incident Response process to ensure timely detection, containment, and recovery from security incidents.

Response Process:

- Security incidents shall be promptly detected through monitoring systems, alerts, and user reporting mechanisms, with proper classification and prioritization
- Affected systems shall be isolated and contained to prevent further spread, data loss, or impact on business operations.
- Detailed investigation and root cause analysis (RCA) shall be conducted, with evidence preservation and audit trails maintained for review

- Systems shall be restored in a controlled manner, ensuring data integrity and validation before resuming normal operations
- All incidents shall be documented and reported to management and relevant authorities, including regulatory reporting where applicable

In the event of a major cyber incident, the organization's Cyber Crisis Management Plan shall be followed.

12. Employee Cyber Security Awareness

Employees are a critical component of the cyber security framework and play a key role in preventing security incidents.

Awareness Measures:

- Employees shall undergo periodic cyber security awareness programs, including simulated phishing exercises to improve identification of malicious emails
- Secure password practices shall be enforced through training on password hygiene, avoidance of reuse, and protection of credentials
- Users shall be educated on safe internet usage, including risks of accessing untrusted websites, downloading unauthorized content, or using public networks
- Reporting of suspicious activity

13. Business Continuity and Disaster Recovery

To ensure operational resilience and continuity of critical business functions, EDC Limited shall implement the following controls:

- Regular backups of critical data shall be maintained with defined retention, secure storage, and availability for recovery during disruptions
- Disaster recovery procedures shall be documented.
- Recovery processes shall be periodically tested through DR drills to validate effectiveness, identify gaps, and ensure timely restoration of services.

14. Review and Updates

This Cyber Security Policy shall be reviewed periodically to ensure its continued relevance and effectiveness. The policy shall be updated whenever significant changes occur in the organization's IT infrastructure, business operations, or regulatory requirements.