EDC LIMITED

A Government of Goa Undertaking

CYBER CRISIS MANAGEMENT PLAN (CCMP) POLICY

SUMMARY OFPOLICY:

Policy Name	Cyber Crisis Management Plan (CCMP) 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 (405thBoard Meeting dated 25/09/2025)

Cyber Crisis Management Plan (CCMP) Policy

1. Purpose

This Cyber Crisis Management Plan (CCMP) Policy outlines the strategic framework for identifying, responding to, managing, and recovering from cyber incidents in a timely and effective manner to protect critical assets of EDC.

2. Objectives

- Ensure effective detection, reporting, containment, and recovery from cyber incidents.
- Minimize impact on operations and reputation.
- Establish clear roles and responsibilities for cyber crisis response.
- Comply with RBI (Reserve Bank of India) and CERT-In (Indian Computer Emergency Response Team) requirements.

3. Scope

This policy applies to all IT infrastructure, networks, data, and applications managed or used by EDC.

4. Cyber Crisis Scenarios

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.

Cyber Crisis Categorization & Recovery Procedures:

A. Server-Related Crisis

Recovery procedure:

1. As soon as incident is identified/detected it should be reported immediately to Computer Cell.
2. Computer Cell shall inform all the HOD's and employees about unavailability of server.
3. Computer Cell shall coordinate with AWS Disaster Recovery to restore the server using techniques such as cross-region snapshot replication.
4. Computer Cell shall also make use of regular data backups maintained to restore the latest data
5. Monitor for residual threats to detect anomalies and suspicious activities, if any.
6. Once the services starts running successfully and server is back online, an intimation to be sent to HODs and employees to start using the server.
7. Loss of data, if any, to be communicated to all employees.
8. CISO categorizes the incident (Low/Medium/High/Critical). Report critical breaches to RBI and relevant authorities.
9. Perform a root cause analysis.
10. Revise policies and procedures if necessary.

Drills and Testing

- Conduct at least **one cyber drill** annually.
- Include employees while performing mock drill scenarios.

B. User systems

Recovery procedure:

1. As soon as incident is identified/detected it should be reported immediately to Computer Cell.
2. Isolate affected/compromised systems and disconnect them from any connected network.
3. Disable affected accounts and reset passwords after threat removal.
4. Analyze root cause using tools and system logs.
5. Re installation of software OS or required applications.
6. Apply necessary patches and remove malicious code.
7. Once the system is ready for use, user to restore their files and folders from **Microsoft OneDrive** application.
8. In case of hardware issues, ensure access continuity via alternate devices.
9. Conduct root cause analysis.
10. Review and revise internal policies if needed.

C. Network-Related Crisis

Recovery procedure:

1. If there is unavailability of network due to reason like hardware, router, or switch failure, then Report network outage immediately to Computer Cell.

2. Computer Cell should inform all the HOD's and Employees about unavailability of specific network.
3. Identify and analyze root cause (e.g., router/switch failure).
4. If internet is down, log complaint with the ISP.
5. Switch ISP from available standby backup connections.
6. Verify network restoration.
7. Notify all users upon network restoration.
8. Conduct a root cause analysis.

Review and Updates

- This policy shall be reviewed whenever significant changes to IT infrastructure are made.

****