Business Continuity and Disaster Recovery Policy

(IT)

24th August 2025

Policy Owner – Bobby Das (Function Head – Technology)

Version 2.3

Purpose

The purpose of the 2COMS Business Continuity and Disaster Recovery Policy is to provide direction and general rules for the creation, implementation, and management of the 2COMS Group IT Department Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

Audience

The 2COMS Business Continuity and Disaster Recovery Policy applies to individuals accountable for ensuring business continuity and disaster recovery processes are developed, supported, tested, and maintained.

Policy Guidelines

Business Continuity

Business Continuity focuses on sustaining the organization's critical business processes during and after a disruption. The Business Continuity Plan (BCP) for IT assets at 2COMS has been fully established, governed, and is actively enforced to ensure the seamless continuation of critical business operations during and after a disruptive event.
The BCP is an integral part of 2COMS' strategy to minimize operational downtime and protect critical IT infrastructure. The plan ensures that all business functions, especially those related to IT assets, are prioritized and protected.

- The BCP is periodically tested and the results should be shared with executive management.
- The BCP is reviewed and updated upon any relevant change to the organization, at the conclusion of plan testing, or least annually.
- The BCP is communicated and distributed to all relevant internal personnel and management.

Business Continuity Planning Framework:

Personnel Safety and Security:
The safety and security of personnel are prioritized above all else. In the event of a disruption, protocols are in place to ensure that personnel can work safely, either remotely or at alternative locations. Emergency procedures have been thoroughly documented, and all staff are trained in their roles and responsibilities during such events.

Management Structure for Preparedness and Response:
A well-defined management structure is in place to prepare for, mitigate, and respond to any disruptive event. The structure includes personnel who have the necessary authority, experience, and competence to manage and make decisions in times of crisis. Regular drills and simulations are conducted to ensure that the response teams can act decisively and efficiently during an incident.

Documented Response and Recovery Procedures:
The BCP includes thoroughly documented plans and procedures for response and recovery. These documents outline the exact steps for managing a disruption, including identification of affected systems, communication with key stakeholders, and restoration of operations. These plans are regularly reviewed and updated to reflect changes in the IT environment and business operations.

BCP Considerations for IT Assets:

The following components have been rigorously implemented and enforced as part of the BCP for IT assets:

- ***Risk Analysis:***
  An internal analysis has been conducted to assess the risks to critical IT business processes and operations with inputs from relevant stakeholders. This includes identifying single points of failure and understanding the potential impact of downtime on the business. The same is reviewed and discussed by the IT Review Team periodically, ensuring that any new risks are identified and mitigated promptly.
- ***Inventory of Critical Systems and Dependencies:***
  An inventory of all critical IT systems and records, along with their dependencies, has been compiled and is regularly updated. This includes hardware, software, applications, data, and communication systems essential to business continuity. Dependencies between systems have been mapped, ensuring that recovery efforts can be coordinated effectively.
- ***Information Security Requirements:***
  Information security is embedded throughout the continuity process. Secure communication protocols, encryption, multi-factor authentication, and data integrity checks are incorporated into the BCP. Data protection measures, such as regular backups and secure offsite storage, are mandated to ensure that sensitive information is safeguarded during a disruption.
- ***Supply Chain Relationships and Critical Infrastructure Support:***
  The BCP includes a comprehensive evaluation of supply chain relationships and their impact on critical IT infrastructure. This involves identifying third-party vendors, cloud service providers (such as AWS and Zoho), and critical service providers. Contingency plans have been put in place to ensure that key suppliers can continue providing services, or alternative arrangements are available if a disruption occurs.
- ***Personnel Safety Processes:***
  The safety of personnel is an integral part of the BCP. A set of processes has been established to ensure that all employees, especially those responsible for IT asset management, are accounted for and have the necessary tools to continue working remotely or from alternate locations if access to business premises is disrupted.

- ***Internal and External Communication Strategies:***
  The BCP includes communication strategies that ensure clear, timely, and effective communication both within the organization and with external stakeholders. This includes predefined templates for emergency notifications, updates for customers, suppliers, and partners, and communication channels for internal teams to coordinate recovery efforts.
- ***Mitigation Strategies and Safeguards:***
  A variety of mitigation strategies have been implemented to reduce the potential impact of disruptions. These include redundant infrastructure (such as cloud services), network security protocols, and system monitoring tools to detect and address issues proactively. Key systems are also configured for high availability, and alternative sites are in place for critical functions.
- ***Contingency Plans for Various Disruption Events:***
  The BCP includes contingency plans for a wide range of disruption scenarios, including but not limited to:
  - *Power failures*
  - *Natural disasters*
  - *Cyber-attacks*
  - *Infrastructure failures*
- ***Plan Testing, Review, and Updates:***
  The BCP undergoes periodic testing to evaluate the effectiveness of recovery procedures. Each test is followed by a review to identify areas for improvement. Test results are submitted to the IT Review Team for evaluation and further refinement of the plan. The BCP is also reviewed and updated annually or after significant changes to the IT infrastructure or business processes.

Disaster Recovery

Disaster Recovery focuses on restoring the technology systems that support both critical and day-to-day business operations.

- 2COMS Group IT Department has implemented this Disaster Recovery Plan ("DRP") to support business objectives outlined in the (BCP/critical processes identified by a Business Impact Analysis).
- The DRP is tested annually, at a minimum.
- The DRP is reviewed and updated upon any relevant change to IT Infrastructure, at the conclusion of plan testing, or least annually.
- The DRP is communicated and distributed to all relevant internal personnel and executive management via official channels and discussed during leadership meets.
- The Disaster Recovery Plan (DRP) for the 2COMS Group IT Department has been fully implemented to ensure the prompt recovery and restoration of critical systems and operations following a disaster. The plan includes the following key components:

- ***Roles and Responsibilities:***
  Clear roles and responsibilities have been defined for the implementation of the DRP. Each team member understands their responsibilities in the event of a disaster, ensuring a coordinated and efficient recovery process.
- ***Risk Identification:***
  A comprehensive list of potential risks to critical systems and sensitive information has been created. This includes all possible disaster scenarios that could affect operations, from cyber-attacks to natural calamities, ensuring preparedness for various disruptions.
- ***Disaster Event Reporting and Escalation Procedures:***
  Detailed procedures are in place for reporting disaster events immediately, with clear escalation steps for rapidly addressing critical issues. This ensures timely recovery of operations and a swift resumption of normal business activities.
- ***Information Security Requirements:***
  Security protocols have been implemented throughout the recovery process to ensure that sensitive data remains protected. This includes encryption, access controls, and secure handling of recovery data during and after the disaster.
- ***Backup and Offsite Storage Inventory:***
  An inventory of all backups and offsite storage locations has been established, ensuring that all mission-critical data is regularly backed up and stored securely offsite. This allows for quick restoration in the event of system failures or data loss.
- ***Contingency Plans for Various Disruption Events:***
  The DRP includes contingency plans for all identified disruption scenarios, from power failures to infrastructure outages. These plans ensure that the organization can continue operations with minimal impact.
- ***Protection and Availability of Plan Documentation:***
  All DRP documentation is securely stored and easily accessible. This includes a disaster recovery manual, emergency contact lists, and recovery steps, ensuring that critical information is available when needed.
- ***Plan Testing, Review, and Updates:***
  The DRP undergoes regular testing as part of a continuous improvement cycle. Each test is followed by a detailed review to identify areas for improvement. The plan is updated quarterly based on the results of these tests and any changes in the IT infrastructure or business requirements.

By implementing these measures, 2COMS ensures that all critical operations are swiftly restored with minimal disruption, allowing for seamless recovery during a disaster event.

Business Continuity and Disaster Recovery Plan (IT) Outline

All data pertinent to the uninterrupted operational transactions for the core business of the 2COMS Group, including but not limited to technical setup data, schema, application framework and live application information is under a composite backup.

All applications are hosted in cloud to have minimum downtime impact due to transactional issues including power, connectivity or system outage at business premises.
Cloud applications are hosted in SaaS model with Global setup with a major base with Zoho Corporation and AWS Cloud. All applications are accessible across the globe from any device connected to the internet.

In the event of disrupted access to business premises or ungovernable scenario such as fire, riot, government initiated curfew or natural calamities any authorized person of the organization will be able to connect with the application via an internet capable device and continue business services with little or no impact on customers or stake holders.

This also safeguards against limited mobility, access or movement due to natural calamities, force majeure or due to government or law enforcement regulations related to movement, transportation or causing limited access to any office premises.

The Disaster Recovery Plan (IT) ensures system recovery and complete backup of mission critical data and structural information.

Summary of Critical Software Development Processes and Their Recovery Priorities:

- AWS EC2 Instance:
    - Critical Software Development Process: Hosting the application and development environment on an AWS EC2 instance.
    - Recovery Priority: High
    - Recovery Plan:
        - Regularly create and maintain Amazon Machine Images (AMIs) of the EC2 instance to facilitate quick restoration.
        - Implement automated backup and restore procedures using AWS services like AWS Backup or custom scripts and file level backups.
        - Use AWS Elastic Load Balancing (ELB) and Auto Scaling to ensure high availability and fault tolerance.

- MySQL Database:
    - Critical Software Development Process: Storing and managing application data in AWS MySQL database.

    - Recovery Priority: High
    - Recovery Plan:
        - Enable automated backups and set an appropriate retention period to recover to a specific point in time.
        - Implement Multi node deployment with auto scaling for high availability and automatic failover in case of a primary database failure.
        - Regularly perform database snapshots to Amazon S3 for additional data protection.
- AWS S3 Files:
    - Critical Software Development Process: Storing and managing application files, code repositories, and backups in Amazon S3.
    - Recovery Priority: Medium
    - Recovery Plan:
        - Enable versioning on S3 buckets to maintain multiple versions of files and recover from accidental deletions or corruptions.
        - Implement cross-region replication for critical data to ensure data redundancy and disaster recovery across AWS regions.
        - Regularly perform data backups to an offsite location or use S3 Object Lock to protect against data tampering.

2COMS has implemented appropriate backup and recovery strategies for all critical components of the software development infrastructure. The Disaster Recovery Plan mandates the development and IT Infrastructure team follows the step-by-step procedures for restoring services for mock tests and in case of catastrophic events. Post regular tests, the team will report to the lead on the status to validate the recovery procedures, to ensure their effectiveness and reduce recovery time during actual disruptions. The development lead will report to the IT Head on the overall recovery and restoration process. Incase any anomalies found, same to be rectified and added to the next test procedure and documented over email.

Application Prioritization and SLA Management

- **Priority Scoring:** Each application and technology asset is assigned a priority score ranging from **1 to 5**, with **5** being the highest. The priority score will reflect the criticality of the application or asset to business operations.
- **SLA for High-Priority Applications:** Applications and technology assets scoring **4** and above are subject to a **Service Level Agreement (SLA)** that mandates full recovery and restoration within **72 business hours or less** following a disruption.
- Applications with priority scores below 4 will be managed based on individual business requirements.

DR Testing and Reporting

- **Quarterly Testing:** A **DR test deployment** will be run quarterly to validate the effectiveness of the recovery procedures and plans. These tests are monitored by the IT Department and reviewed by the **IT Review Team**.
- **Test Reporting:** After each test, detailed results, including any challenges encountered and corrective actions taken, will be submitted to the IT Review Team. Any improvements or modifications to the plan will be documented and integrated into future tests.

Waivers

Waivers from certain policy provisions may be sought following the 2COMS Group IT Department Waiver Process by informing the IT Head and the Management over email and getting written approval.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any involved party found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s) or employment, and related civil or criminal penalties.

Review

This policy and plan document to be reviewed and updated atleast once annually.