iMocha	Business Continuity and Disaster Recovery Plan

Version Control

Current Version	**1.2**
Released on:	**1-Sept-2025**
Classification	**Internal Use**

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	1-Sept-2022	Initial version	Wasim Shaikh	Sujit Karpe
1.1	1-Sept-2023	Second version	Nishant Thool	Sujit Karpe
1.2	1-Sept-2024	Third version	Nishant Thool	Sujit Karpe
1.2	1-Sept-2025	Fourth version	Nishant Thool	Sujit Karpe

Business Continuity and Disaster Recovery Plan

1. SCOPE

This plan applies to all iMocha assets utilized by employees and contractors acting on behalf of iMocha or accessing its applications, infrastructure, systems, or data. All employees and contractors are required to read, accept, and follow all iMocha policies and plans.

Scope for Mission Critical Services

Mission critical services and systems are those required for the functioning of the iMocha product(s). Mission Critical services and systems include critical production systems required for immediate recovery, services affecting the engineering team's ability to support production operations and product development, and the ability to support iMocha customers.

All essential data is typically stored remotely using commercial cloud providers with proper backup and redundancy processes in place. This approach is subject to change and designed to minimize any disruption from physical incidents or disasters.

2. PURPOSE

This Business Continuity and Disaster Recovery Plan guides iMocha in the event of a significant business disaster or other disruption to normal service. iMocha must respond to business disasters and disruption by safeguarding employees' lives and company assets, making a financial and operational assessment, securing data, and quickly recovering operations.

This plan applies to all iMocha assets utilized by employees and contractors acting on behalf of iMocha or accessing its applications, infrastructure, systems, or data. All employees and contractors are required to read, accept, and follow all iMocha policies and plans.

3. POLICY

3.1 System Outages

Planned Outage
From time to time, iMocha may distribute a service update to all affected users prior to planned downtime.

Unplanned Outage
All unplanned outages should be treated as an incident; security@imocha.io and the executive team should be immediately emailed and notified of any unplanned outage.

3.2 Expectations

Alternate Physical Location(s) of Employees
In the event of an internal disaster that affects a iMocha office location, all team members will be moved from such affected offices to each member's respective home or an alternate location to work remotely.

Reliance on Third-Party Services
iMocha utilizes and relies on mission critical third-party cloud services. In the event of a significant business disaster, iMocha will quickly work to establish alternative arrangements if a mission critical vendor can no longer provide the needed services or goods.

Mission critical third-party vendors include:

This plan depends on the likelihood that:

- Remote work can continue to take place in the event of a disaster; and
- Mission critical vendor services, and essential iMocha services, systems, and data can still be made available or alternative solutions can be implemented (including backups and services provided by such third-party vendors)

3.3 Priorities

In the event of a disaster affecting iMocha essential systems or its team members, Sujit Karpe will oversee and respond in accordance with this Plan and will initiate specific actions for recovery.
The priorities during a business disaster are to:

- Secure the safety of team members and visitors;
- Mitigate threats or limit the damage that threats can cause to iMocha, its team, and its customers; and
- Ensure that essential business functions can continue or determine what is required to restart essential business functions

3.4 Backup and Retention

All vital data that would be affected by disruption are maintained and controlled by the data's applicable teams.
In the event of a facility disruption, critical records located in such a facility may be destroyed or inaccessible. The number of critical records, which would have to be reconstructed, will depend on when the last transfer of critical records to the cloud storage location occurred.

Backup Requirements

- Database backups must be performed
- Backups must be retained for at least 30 days
- The maximum allowable retention period for a database backup should be determined base on regulatory and contractual requirements
- Backups are periodically tested to ensure that backups are sufficient and reliable in accordance with this plan
- Backup systems and media protect the availability of stored data.

3.5 Alternate Communications

The organization may communicate using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.

In the event of a significant business disaster, an assessment will be conducted to determine which means of communication are still available. These means of communication will then be utilized to communicate with personnel, customers, partners and other third-parties.

Testing

Testing the plan is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by Sujit Karpe and any designee. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods noted in the subsections below.

Walkthroughs

Team members must walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with all relevant stakeholders and familiarize them with procedures, equipment, offsite facilities, and recovery efforts in preparation of a business disaster or disruption.

Table Top Exercises

Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test.

Personnel involved with business continuity must utilize validated checklists to provide a reasonable level of assurance for many disaster scenarios. These personnel must analyze the output of the

previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

3.6 Business Continuity and Disaster Recovery Stages

This Plan divides recovery into three stages: Disaster, Response, and Recovery.

Declaring a disaster is the responsibility of senior management. Since it is almost impossible to predict when and how a disaster might occur, iMocha and its team members must be prepared to monitor and signal a disaster to management from:

- First hand observation
- Security applications
- Network monitoring and logging tools
- Environmental and security alarms
- Team members
- Customers
- Partners
- Vendors
- Media

Disaster Stage
If a disaster has been declared, this Plan and any related responses would go into effect.

The disaster stage may include the following processes:

- Senior management declares the disaster, and
- Notifies management and appropriate team members to create the appropriate Disaster Recovery Team (DRT),
- DRT initiates internal and external communication lines, and communicate to the following parties as appropriate:
- General Counsel
- Authorities
- Personnel
- Customers
- Vendors, third-parties, and other applicable stakeholders
- DRT determines appropriate emergency response measures

Response Stage

In this phase, the team determines what team members, facilities and customer deployments are affected by the disaster scenario and in what way they are affected by performing an impact assessment.

This stage continues until an alternate facility location and/or essential business and production functions are established and services restored. If non-essential functions are affected, essential functions may be prioritized during a disaster event.

The response stage may include the following processes:

- Execution of a business impact assessment,
- Relocation to an alternative facility or establish work from home requirements,
- Verification and/or backing up of affected data and systems, and
- Restoration of essential iMocha services

Recovery Stage

Recovery begins with the activities necessary to return to business as usual including re-establishing the primary facility. For engineering, this stage begins with the restoration of iMocha services in an available commercial cloud provider's region. Recovery time objectives (RTOs) and recovery point objectives (RPOs) are to be defined when relevant for applicable systems.

Key Learning Stage

As soon as possible, iMocha senior management must meet with the DRT and other stakeholders for a post-mortem review to better understand the disaster event that took place and how it and others may be prevented in the future.

The retrospective must be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Lessons learned during the disaster must be captured within the post-mortem review and incorporated as updates into existing documentation.

3.7 Exceptions

iMocha business needs, local situations, laws, and regulations may occasionally call for an exception to this policy or any other iMocha policy. If an exception is needed, iMocha management will determine an acceptable alternative approach.

3.8 Enforcements

Any violation of this policy or any other iMocha policy or procedure may result in disciplinary action, up to and including termination of employment. iMocha reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. iMocha does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any personnel who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of iMocha as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

3.9 Responsibility, Review and Audit

iMocha reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Sujit Karpe.

This document was last updated on 01/09/2025.