SATYA MICROCAPITAL LIMITED

IT Business Continuity and Disaster Recovery Policy and Procedure

Version 1.0

November 2023

Table of Contents

1. Purpose **3**

2. Scope **3**

3. Policy **3**

3.1 Policy Statements **3**

IT Business Continuity and Disaster Recovery Policy and Procedure

1. Purpose

The purpose of this policy is to establish necessary controls for maintaining IT Business Continuity and DR Plan for critical business process information and it's supporting IT assets, technology supported and IT resources within ORGANIZATION's Infrastructure.

2. Scope

This policy applies to identified critical IT assets, applications and its supporting IT facilities owned or managed by organization.

3. Policy

- The IT Business Continuity and Disaster Recovery Policy shall ensure that critical IT infrastructure needed for meeting business requirements are maintained with minimal interruption in event of disaster and failures.
- Application systems and business processes that are critical to the business shall be planned for resiliency of operations in the event of business disruptions.
- The cost to benefit analysis for purpose of countermeasures to be implemented shall be considered and continually reviewed as part of normal management responsibility.
- Major business continuity risks that threaten the continuation of the delivery of critical services shall be identified, and an effective preventative, detective and responsive recovery strategies shall be developed, implemented, tested and maintained.
- The BCP and IT DR policy shall help ORGANIZATION's business teams, IT team and users in responding to business continuity risks.

3.1 Policy Statements

3.1.1 IT Business Continuity and Disaster Recovery

- ORGANIZATION's respective stakeholders are responsible for assessing the potential impact that loss of data would have on their business processes and shall derive acceptable RPO/RTO values.
- The plans shall include provisions for business continuity of critical business process and recovery in the event of disaster and failures.
- Plan shall contain considerations of backups of critical information supporting these business operations based on Business Impact and Risk Assessment in line with respective department's RPO/RTO values.
- IT Business impact analysis (BIA) shall be performed for critical applications along with the risk assessment as and when appropriate.
- The following shall be considered while implementing any BCP/DR program:
    - Identify critical business applications, IT infra and supporting technologies.
    - Develop an appropriate cost-effective recovery strategy.
    - Identify alternate, backup locations with the necessary infrastructure to support the recovery needs.
    - Identify the management and membership of the disaster response and recovery teams.

- Identify the required recovery actions, identify and ensure the availability of required IT resources, and compile this information
- Train the recovery teams in the performance of their specific tasks.
- Identify vendor recovery support capability (if any);

- Whiteboard walkthrough or an actual simulation test of all IT business continuity plan/disaster recovery plans shall be conducted as and when appropriate, or at least on an annual basis.

3.1.2 Recovery strategy/ Contingency Plan

- Critical IT process / asset and supporting infrastructure and physical location shall have a recovery strategy/contingency plan.
- To the extent practical and feasible, business contingency and IT DR Contingency plans shall be tested at regular intervals and records be maintained.
- The roles and responsibilities for business contingency and IT DR Contingency plans must be reviewed and updated as and when appropriate or at least on an annual basis
- Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.
- In order to protect against cyber-attacks a Cyber Crisis Management Plan (CCMP) shall be created as part of the ORGANIZATION's approved overall strategy.
- The CCMP shall be capable of addressing detection, response, recovery and containment strategies, this plan should be designed, implemented tested, monitored and maintained.