BUSINESS CONTINUITY CUM DISASTER RISK MANAGEMENT POLICY

KUSHAL FINNOVATION CAPITAL PRIVATE LIMITED

Version	Date	Reviewer	Approver	Document Changes
4.0	June 23, 2025	Department of Information Technology	Board of Directors	Amendments and Revisions in the Policy
3.0	May 29, 2024	Department of Information Technology	Board of Directors	Amendments and Revisions in the Policy
2.0	March 31, 2023	Department of Information Technology	Board of Directors	Amendments and Revisions in the Policy
1.0	December 7, 2022	Department of Information Technology	Board of Directors	Implementation of Policy

Table of Contents

Objective

The objective of this Business Continuity cum Disaster Risk Management Policy is to ensure continuity of critical Business operations and IT operations that are necessary for conducting Business during disaster and minimize the disruption of critical operations to near zero level by putting in place a robust and resilient business continuity strategy and framework while meeting Regulatory and compliance requirements.

Definitions

Business Continuity: Ongoing process to ensure that necessary steps are taken to identify the threats of potential losses and maintain viable mitigation strategies, recovery plans, and continuity of services.

Business Continuity / Disaster Recovery Manager: Coordinates planning and implementation for the overall recovery of the organization or business units.

Business Continuity / Disaster Management Planning Team: Responsible for planning, developing, and implementing business continuity-related plans and projects.

Business Continuity / Disaster Management Steering Committee: Provides direction, advice, guidance, and financial approval for BC/DR programs.

Business Unit: A group of individuals organised to perform specific duties based on the functions performed within the organisation. Examples of business units are Finance, Operations, Applications Development, Client Technologies, Network Data Services, etc.

Crisis Management Team (CMT): Senior managers from each functional area (usually the BC/DR Steering Committee members) are responsible for developing and implementing a comprehensive plan for responding to a disaster.

Disaster Management (DM): The technical aspect of Business Continuity. The collection of resources and activities to re-establish IT services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption. Disaster recovery includes subsequent resumption and restoration of operations at a more permanent site.

Disaster Management Team(s) (DMT): A team (or teams) directed by the CMT to respond to a disaster. Can be comprised of multifunctional team members or divided into multiple specialty teams depending on the scope of the disaster. Led by the DMT leader (as appointed by the CMT).

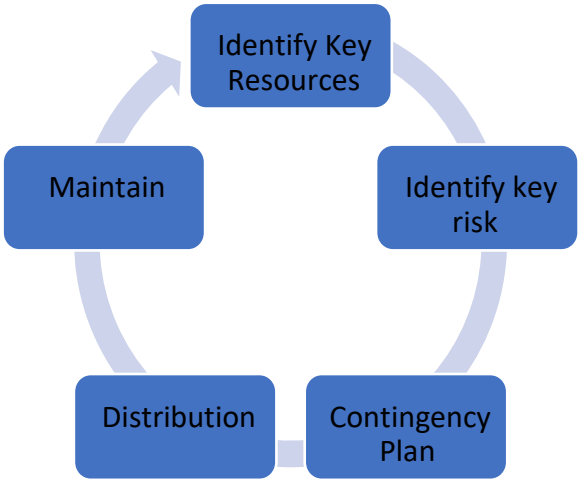
Disaster Site: The Disaster Site shall be the registered office of the Company and such other offices as opened by the Company from time to time. Presently, the registered office of the Company is situated at Condor Vista #5, 2nd Floor Block 2A Left wing, Near Anjappar Chettinad Restaurant, 4th B Block, 100 FT Road, Koramangala, Bangalore 560034.

Purpose

- The Company, like any other entity, is exposed to potential risks that could disrupt or destroy critical business functions. Our strategy for continuing business in the event of an incident is to ensure the safety and security of all employees and to continue critical business functions. The purpose of the

BC/DRM policy is to ensure that all Company business activities can be kept at normal or near normal performance following an incident that has the potential to disrupt or destroy the Company.

- Protection of Company systems and software
- Adequately train personnel in disaster preparedness and evacuation procedures
- Ensure that the plan is tested periodically and at least once annually.
- Meet at least annually to review and update the plan.
- Periodically report findings to the Board for review.
- Evaluate the KFCPL's insurance coverage to ensure that it is up-to-date and adequate for current needs.



Relocation Strategy

In the event of a disaster or disruption to the office facilities, the strategy is to resume operations from the alternative coworking space, as stated in the Business Continuity Plan.

BCDRM Committee

In the event of a disaster or disruption of services, the BCDRM Committee shall convene and decide on implementation of BCRDM Strategy. Annual Maintenance Contract (AMC) should be diarised and reviewed quarterly by the BCDRM Committee, as per the Business Continuity Plan. The minutes of the BCDRM Committee meeting to be submitted to the Board on quarterly basis, 'NIL' report to be submitted if there are cases of disaster.

Restoration of Hard Copy Files & Documents

In the event of a disaster or disruption of the hardcopy of records/documents, all the documents are digitally stored on the cloud and would be recovered from the cloud and based on the criticality the documents will be reconstructed or get the certified copy of the same from the party.

Restoration of the Software Application /Digital Records / Transaction details

In the event of a disaster the files are all securely stored in the virtual private cloud on AWS / DO, which would be recovered easily with the secured authentication techniques.

Restoration of the Computer Systems / Laptops

In the event of a facility disruption, the IT disaster plan strategy will be to back up all the files on VPC and restore them whenever needed with user authentication.

Employee Training

Employees training plays a vital role during the incident or disaster. Employees that have roles defined in the plan will be trained to carry out the individual responsibilities. The response team will be integrated in the plan, updating processes and make recommendations of the most effective approach to the disaster response. Basic training & understanding of the business continuity will be provided to all the employees.

- Executives are given a high-level overview of the BCDRM.
- Functional managers are given an overview and a more concentrated BCDRM.
- Employees will be given an overview of BCDRM and their contribution. Conducting drills along with the department head.

Disaster Threats, Its Impact and Threat Mitigation plan

1.0 Facility Threats

Threat Identification	Description	Threat Triggers	Threat Impact	Threat Mitigation	Constraints Identified	Threat Controls	Likelihood of Threat Occurring	Impact Level
Severe Weather	Flooding, flying objects and falling trees.	Storm, Wind	All personnel, vehicles & Public transportation	Watch weather report, park the vehicles in non-flood area & stay inside.	Out of human control, no time of event to occur, public transportation.	Parking area to be air marked and bad weather forecast to be communicated for better planning.	High	Moderate
Bomb Threat	Explosion may lead to loss of life, Structural damage of workspace.	Terrorist	Office building and surrounding neighbourhood.	Immediate evacuation and security are informed.	No Drills;	Evacuation & identification of suspicious objects training & drill.	Low	Catastrophic
Power Outage	Loss of work in progress. Lost time, building access, AC & Lighting	Electricity board power outage - unable to supply electricity. Downed power line due to natural disaster, transformer failure.	Some employees in the affected building due to hard restart of the equipment. No Wi-Fi availability due to power outage.	Brief leadership and business partners.	There is no power backup. for the building during the power outage. If cell battery is drained, communication will be impacted.	On site UPS with 10 mins back up is available for the user desktop.	Medium	Moderate
Water Outage	Fire Hazards, Unsanitary conditions and lack of drinking water	Internal water supply failure: water supply cut from city municipal corporation.	Employees in the affected facility will be impacted by potential fire hazard, lack of restroom. facilities, and RO drinking water.	Keep bottled water as backup & shut down certain non-critical process.	None	Contract relationship with the facility. manager, other water supplier and plumbing contractor. Office boy	Low	Moderate

						with the vehicle and petty cash for pick-up of bottled water.		
Building fire	Uncontrolled fire in the building & transportation corridors or accidental building fire impacting the personnel in the affected area. Impact of loss of business documents, important physical contracts, Loan Agreements, vendor agreement, PDCs, Corporate guarantee like Bonds / PDCs.	Faulty equipment, overloaded circuits, accidents.	Occupied facility, breathing, loss of time, potential asset loss.	Fire Control mechanism kits easily accessible. Evacuation of the building facility. Outside resources for the restoration of the facility. Communication to the leadership about the estimate of the time for out of-service and alternate work plan.	Conditions out of control.	Evacuation drills held. Fire extinguishers located within the facility and corridors and their expiry dates diarised and ensured that they are in force. Fire exit path signages, Emergency list of outside resources displayed at the all the fire exit way.	Medium	Significant
Burglary / Theft	Loss of company assets, material and public property. Impact to product development schedule and delivery.	Thieves	Company financial loss and personnel loss.	Repair the physical breach and Report loss to local authorities.	No asset tracking mechanism.	Security guards to deter theft, security cameras, door access controls.	Medium	Moderate

2.0 Information Security Threats

Threat Identification	Description	Threat Triggers	Threat Impact	Threat Mitigation	Constraints Identified	Threat Controls	Likelihood of Threat Occurring	Impact Level
Cyber Threat	Absent or deficient prevention and security measures employed to provide reasonable level of security of data, system and IT infrastructure, which includes security from illegal penetration into the system, loss or attack by cyber attackers. Also access where systems / applications / physical locations are not set up to restrict access to individual attempting to gain illegal entry.	Introduction of malware by mistake or internally by insider. Compromised systems may cause vulnerabilities that exploits the system.	Company, partners of company, or individuals and all departments. The impact will depend up to the type of malware and recovery time.	1. Professional antivirus for the protection of end points and client machines. 2. Implementation of ISMS guidelines and policies throughout the organization. 3. Continuous evaluation and implementation of IT security offerings available in the market. 4. Identify the IT security personnel 5. Adoption of penetration tests and monitoring of the security level issues and fixing them from time-to-time. 6. Changing the password of the client or entry points. 7. Provide closed loop secured network for IT team members to work from home.	None	1. Implementation of IT security policies and review of same on regular intervals to revise the same. 2. Adoption of the ISO 270001 practices by April, 2023. 3. Implementation of VPN for remote working to avoid critical systems exposure to public network. 4. Conducting annual risk assessment of the system. 5. Monitor the logs on regular basis to identify the possible treat attacks and take counter measures to block them. 6. Implement geo fencing to avoid the using of client application in other countries to avoid vulnerability issues.	High	Significant

3.0 Legal Threats

Threat Identification	Description	Threat Triggers	Threat Impact	Threat Mitigation	Constraints Identified	Threat Controls	Likelihood of Threat Occuring	Impact Level
Non compliance monitoring	Internal stakeholders may monitor ethics and compliance programs as a set of check-the box activities or event worse, as bottlenecks to achieve the business objectives.	None	Impact on partnerships, business corporations, stakeholders and Investors	Maker-Checker process for all the compliance related, to avoid the noncompliance.	1. Unclear objectives 2. Unrealistic deadlines 3. Ownership and responsibility 4. Policies existence and implementation 5. Lack of followup 6. One-time process	None	Medium	Significant
Operational Risk	Failure of effective resource management.	Improper resource management, no clear roles and responsibilities, day to-day activities tracking, field force management as there is no visibility.	Impact on partnerships, business corporations, stakeholders and Investors	Incorporation of resource monitoring tool.	1. Unclear objectives 2. Onboarding training of new resources 3. Access to right contacts with the organization 4. Ownership 5. Lack of follow-up 6. Lack of monitoring 7. Review of resources on regular basis	None	Medium	Moderate
Antitrust Competition	1. Risks arrising due to market competition in the industry. 2. Company specific	1. Contract with suppliers / contractors. 2. Understanding of exclusivity and share product segment 3. Price	Impact on partnerships, business corporations, stakeholder	Legal vetting and business contracts review.	1. Unclear expectations 2. Unrealistic deadlines 3. Access to policy document and awareness of	1. Educate employees, deter risky conducts and set a culture to report the	Medium	Significant

	intellectual property and importance. 3. Use of suppliers / contractors and their interaction with competitors.	and business presentations 4.	s and Investors		the policy guidelines 4. Lack of followup 5. One-time activity	potential issues. 2. Mandatory employee training by the knowledgea ble person 3. Training should be in person / web based		

4.0 Social Media Threats

Threat Identification	Description	Threat Triggers	Threat Impact	Threat Mitigation	Constraints Identified	Threat Controls	Likelihood of Threat Occurring	Impact Level
Social media & unauthorized Representation	1. Negative comments about the company 2. Disclosures of proprietary information 3. Exposure of personnel identifying information 4. Fraud 5. information leakage 8. Data loss 9. privacy and infringement 10. Corporate Espionage 11. Reconnaissance 12. content management	Employees contacting social media and decides to release sensitive information unintentionally or intentionally.	Internal and external stakeholders are affected due to negativity surrounding rumours by 'Legit' former of current employees.	Employees to sign a non-disclosure agreement when onboarding. Employees have background checks and are authorized to proprietary Assets on a need-to-know basis.	None	To create an easily understandable social media policy and guidelines.	high	Significant

	13. content taxonomy 14 Employees who engage in "off the record" conversation and those that gives unauthorized interviews with reporters. this can have negative impact on organization.							

5.0 Accidental Threats

Threat Identification	Description	Threst Triggers	Threat Impact	Threat Mitigation	Constrains Identified	Threat Controls	Likelihood of Threat Occuring	Impact Level
Accidental Employee Loss	Traveling to different location, meetings, business partner meetings	Travel accident, fall or any.	Co-workers, external stakeholders & operations.	None	Uncontrolled environment	Mandatory submission of Driving License during joining, Policy for safe travel to be established.	Medium	Moderate