IRDAI REGISTERED INSURANCE BROKER

Business Continuity and Disaster Recovery Policy

Document Number: SMCInsurance/PO- 06

Document Details

Title	Business Continuity and Disaster Recovery Policy
Version	0.1
Author	IT- Team
Classification	Internal
Reviewer & Custodian	Director
Approved By	Director

Distribution List

Name
Internal Distribution Only

Version History

Version Number	**Version Date**	**Change Description**
3.1	8-06-2020	New policy creation

SMC INSURANCE BROKERS PVT. LTD.

Table of Contents

Contents

1. Overview

Smc Insurance Brokers Private Limited (hereafter, SMC) is susceptible to operational disruptions caused by internal and external threats such as fire, earthquakes, wars, terrorist attacks, system failures, etc. such disasters may lead to severe operational disruptions and sometimes threaten the solvency, and business continuity of SMC, which could adversely impact the financial system as a whole. In today's world, Business Continuity Plan (BCP) and Disaster Recovery Plan are becoming increasingly important.

Business Continuity Planning (BCP) is an ongoing process requiring full support and commitment of the Top Management. Business Continuity Plan (BCP) forms a part of SMC' overall Business Continuity Management (BCM) Plan, which is the preparedness of SMC, including policies, standards, and procedures to ensure continuity, resumption, and recovery of critical business processes at agreed levels, and the limit of impact of disaster on infrastructure (including IT), people, and processes are minimized, or to minimize the operation, financial, reputational, legal, and other material consequences arising from such consequences. The primary objective of BCP is to maintain viable recovery strategies and plans to ensure that all critical information/ data are salvaged in the minimum possible time in the event of a major incident which may threaten or disrupt normal operations or services for sufficient time to significantly affect, or cause failure of essential services rendered by SMC. BCP will look into the following areas:

- Availability of servers used for {DR Server};
- Availability of network resources for keeping the business applications going on;
- Availability of intranet servers;
- Availability of physical premises for employees.

For Business as a whole, all the possible threats along with their probability and impact on business are considered in Risk Assessment Document.

2. Policy Review, Revision and Communication

This policy shall be reviewed and updated once every year to incorporate relevant changes. All subsequent updates to the policy shall be communicated over E-mail and made available on intranet to all employees by the end of March every year.

SMC INSURANCE BROKERS PVT. LTD.

3. Purpose

- The purpose of this policy is to implement and maintain SMC resilience to disruption, interruption, or loss in providing critical services in the event of a major operational disruption.
- The policy also serves to provide an appropriate framework to facilitate SMC compliance with legal and regulatory requirements.
- Business Continuity refers to the activities required to keep SMC running during a period of displacement, or interruption of normal operation. Whereas, Disaster Recovery (DR) is the process of rebuilding the operation or infrastructure after the disaster has occurred.
- Business Continuity Plan (BCP) includes planning for Disaster Recovery. Disaster might occur anytime so, SMC must be prepared.
- Business Continuity Plan shall cover the occurrence of following events:
    - Equipment failure (such as disk crash);
    - Disruption of power supply or telecommunication;
    - Application failure or corruption of database;
    - Human error, sabotages or strike;
    - Malicious Software (Viruses, Worms, Trojan horses) attack;
    - Hacking or other Internet attacks;
    - Social unrest or terrorist attacks;
    - Fire;
    - Natural disasters (Flood, Earthquake, Hurricanes etc.)
- The underlying purpose of Business Continuity Planning is the speedy resumption of business operations; hence, it is essential to consider the entire SMC, not just the information systems processing services, while developing a plan. BCP Project shall be initiated, and formally approved, and committed by the Management.

4. Business Recovery

This is the process where a business area has to relocate to another location as a result of a major incident or event that prevents use of a premises, or region, or country also, it may require Disaster Recovery to support it. SMC has its Data Center is location at (Delhi) and Disaster Recovery Site is located at (Mumbai). In case of any disaster, SMC can easily move to DR location ready with all infrastructures.

- **Backup**
  - Backup is taken on a dedicated server as per Backup Policy and Procedure.
- **Network**
  - SMC has basic infrastructure available at (Mumbai). In case of problem in any 1 (one) switch, same can be shifted in minimum time frame to another switch resulting in minimum downtime. All networking components are also as per the very best in industry standards and SMC uses networking equipment only from (TCL and Airtel).
- **Security**
  - SMC network has several placed devices at all entry points for safe and limited access. This ensures that all users for any application/ server are authorized and authenticated. SMC network has Intrusion detection system which is placed inside firewall, and through devices public facing server farm, and backend Internal LAN connections in promiscuous mode through which there is monitoring to prevent any unauthorized access, or online attacks through (DHCP/ MAC filtering) in the production Data Centers (DC).
  - In addition to all the security measures, Anti- Virus is installed on all desktops, and laptops.
- **Servers**
  - There is active directory system in place for safe authentication of the desktops, and all the machines logged in a domain controller environment. Periodic patching of machines is being done and strictly monitored through manage engine system hosted internally.
- **Data Backup and Recovery**
  - SMC data backup and recovery policies and procedures are documented in Backup Policy and Procedure.

- Proposed backup for primary site is as follows:
  - Operating System level, backup will be provided for all servers (4 hours) by default;
  - Total Data to be backed up: (10) GB;
  - Backup size, schedule, and retention policy will be as follows:
    - Source data;
    - incremental changes;
    - Backup schedule:
      - ✓ Daily incremental with 7 (seven) days retention;
      - ✓ Weekly full with 4 (four) weeks retention.

- **Prevention of Electric Power Outage**
  - Electrical power outages are 1 (one) of the biggest reasons for data loss. SMC has a dual-level backup power supply mechanism in place.
  - This dual- level backup consists of:
    - Multiple UPS to servers (will forms first level of backup);
    - Dual diesel generators to servers (will forms second level of backup).

5. Business Impact Analysis

- Business Impact Analysis (BIA) is intended to identify the impacts from disruptions to the critical business services identified.
- The purpose of BIA is to:
  - Identify service offerings, and its criticality levels for all functions/ services;
  - Establish, and estimate the maximum tolerable downtime for each service;
  - Assess the impact of incidents;
  - Determine the priorities, and processes for recovery of critical business processes.

- Business Impact Analysis begins with the categorization of the identified critical services into 4 (four) categories, i.e. critical functions, essential functions, necessary functions, and desirable functions.
- The guidelines for categorization are given below:

SMC INSURANCE BROKERS PVT. LTD.

Sr. No.	Criteria	Description	Recovery Time Frame
1	Critical functions	If these business functions are interrupted or unavailable for some time, it can completely jeopardize the business, and cause heavy damages to the business.	**100% of the services in 6 hours.**
2	Essential functions	Those functions, whose loss would seriously affect SMC's ability to function for long.	**100% of the services in 6 hours..**
3	Necessary functions	SMC can continue functioning; however, absence of these functions would limit their effectiveness, to a great extent.	**100% of the services in 6 hours..**
4	Desirable functions (Good practices)	These functions would be beneficial; however, their absence would not affect the capability of SMC.	**100% of the services in 6 hours..**

- We have proper backups of all the servers, and databases, multiple ISP connectivity with failover plans. Judging the DR and BCP in a nut shell is covering each and every aspect of the operation of the business, and proving a guarantee to overcome the disaster and continue the business.

6. Responsibility

Business Continuity Team shall be headed by CISO; who shall be the Owner, and shall look overall implementation of the Business Continuity Plan. He shall be assisted by BCP Team.

7. Key Roles

Escalation hierarchy of the DR Team is a management responsibility. This section describes the key roles of the:

- **Senior Management:**
  - Senior management under the standard of due care, and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess, and incorporate results of the risk assessment activity into the decision- making process.

    An effective risk management program that assesses, and mitigates IT- related mission risks requires the support, and involvement of Senior Management;

- Senior Management shall nominate another Senior Executive as an alternate Team Leader to take the ownership of BCP; in the absence of the Owner, he/ she will be vested with the power of declaring a disaster;
- Senior Management shall be responsible for:
  - Identifying the Team Members for BCP;
  - Developing, and implementing the BCP;
  - Declaring a disaster, and activating the BCP Team;
  - Minimizing the impact of the Incident/ Disaster Event, and recovering the identified critical assets as per the Business Continuity Plan;
  - Providing training to Team Members;
  - Testing and keeping BCP up- to- date.

- **System and Information Owners:**
  - System and Information Owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically, System and Information Owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign- off on changes to their IT systems (e.g., system enhancement, major changes to the software, and hardware). System and Information Owners must therefore, understand their role in the risk management process and fully support this process.

- **IT Security Practitioners:**
  - IT security practitioners (e.g., network, system, application and database administrators, computer specialists, security analysts, security consultants) are responsible for proper implementation of security requirements in their IT systems.
  - As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure, SMC' policies and introduction of new technologies). IT security practitioners must support, or use the risk management process to identify, and assess new potential risks and implement new security controls as needed to safeguard their IT systems.
  -

- **Security Awareness Trainers (Security/ Subject Matter Professionals):**

SMC INSURANCE BROKERS PVT. LTD.

- SMC personnel are the users of IT system. Use of IT systems and data according to SMC policies, guidelines and rules of behavior is critical to mitigate risk and protect SMC IT resources. To minimize risk to IT systems, it is essential that system and application users to be provided with security awareness training.
- Therefore, IT Security Trainers, or Security/ Subject Matter Professionals must understand the risk management process so that they can develop appropriate training materials, and incorporate risk assessment into training programs to educate end- users.

- **Implementation**

  - Asset Owner shall define the Maximum Acceptable Outage i.e. the maximum time during which the business shall not be affected. The asset owner shall define the Recovery Time Objective (RTO) for the asset to define appropriate recovery architecture for the asset. The asset owner shall ensure that appropriate Recovery Architecture is defined, so that the asset can be recovered within the Recovery Time Objective.
  - Asset Owner shall ensure that the recovery architecture and backup requirements are implemented as defined. Asset Owner and IT shall define the sequence, and priority for the recovery from disaster. Recovery architecture shall also define the process to restore the assets to their normal production environment.

8. Capacity Management

Use of information and information facility resources should be appropriately monitored, and projections made of future capacity requirements to ensure adequate systems performance. Control includes:

- Identification of capacity requirements for each new and ongoing system/ service.
- Projection of future capacity requirements, taking into account current use, projected trends, and anticipated changes in business requirements.
- System monitoring and tuning to ensure (wherever possible) and improve the availability and effectiveness of current system.
- Analysis will be carried out on a quarterly basis.
- Records will be maintained for 3 (three) months.
- Capacity planning will be analyzed for identified production data center devices.
- IT- Head along with Operations Head will decide on taking required decision on upgrading services/ capacities depending on future projections.

SMC INSURANCE BROKERS PVT. LTD.

- In order to achieve capacity planning management, IT- Team reports utilization parameters to CISO like CPU Utilization, Memory Utilization and Disk Utilization for identified devices and servers. Additional resources are added as per below matrix:

Windows Servers		
CPU	**Memory**	**Disk Usage**
>60% for continuous 2 weeks	>80% for continuous 2 weeks	>90% for continuous 2 weeks

- **Template to monitor Capacity of Critical Servers**

Date	Server IP Address/ Name			Server IP Address/ Name			Server IP Address/ Name		
	CPU	Memory	Disk Usage	CPU	Memory	Disk Usage	CPU	Memory	Disk Usage

9. BCP Testing

- A proper test plan shall be finalized, and implemented as, and when required, or at least once in a year to ensure its proper functionality, and training to the BC Team Members. The BC Test Plan shall specify:
  - The type of test;
  - The expected period of recovery;
  - Frequency for such tests.
- The results of the BC tests shall be documented, and used for fine tuning the BCP. The following are the testing type and schedules:
  - Link Failover Testing- 6 (six) Month;
  - One structured walk- through Every Quarter for all the critical devices;
  - Fire Evacuation Drills- Annually;
  - Table top testing for Critical Servers;
  - Table top testing for Web servers;
  - Table top testing for Database.
- In case of a security incident, or emergency, please contact any of the following:

Serial No.	Members	Phone Numbers
1	IT Head	9818203275

10. Disaster Recovery

SMC INSURANCE BROKERS PVT. LTD.

Disaster Recovery encompasses all aspects of technology recovery during a major incident, or event affecting the normal operations of SMC.

10.1. Scenario: Fire/ Explosion Facility/ Infrastructure not available

This can be due to bursting of UPS batteries in case of over- heating; short circuit on account of ageing of wires/ poor cable joint.

- **Preparedness:**
  - Fire equipment's are checked, and fire evacuation mock drill conducted periodically Emergency phone numbers of fire, police, ambulance, hospitals available ACs are installed as required. Employees provided with firefighting techniques.
- **Pre- Declaration Activities:**
  - Direct all operations to stop within the affected area taking into consideration priorities for safety of personnel, minimize damage to property, Environment, and minimize loss of materials.
  - All workers/ staff of the areas affected are evacuated to the appropriate assembly points. To provide advice, and information to the Fire, Security Officers, and the local Fire Service Emergency Shutdown of all power equipment's, AC, and critical servers.
- **Recovery Activities:**
  - IT equipment's, and important filing papers are moved to a safer location inside the premises, under close observation of trained fire wardens, use fire extinguisher where possible to contain Fire Contact. Fire Department Assess damage when fire is contained restore seating space, computer provisioning, and network connectivity Inform employees when setup is restored.

10.2. Scenario: Earthquake

- **Preparedness:**
  - Building is earthquake resistant;
  - Evacuation drill performed periodically.

- **Pre- Declaration Activities:**
  - Direct all operations to stop within the affected area taking in to consideration priorities for safety of personnel, minimize damage to property, environment, and minimize loss of materials. All workers/ staff of the areas affected are evacuated to the appropriate assembly points to provide advice, and information to the Fire, Security officers, and the local fire service. Emergency Shutdown of all power equipment, AC, and critical servers.

- **Recovery Activities:**
  - Recover all information, and information processing devices Admin to locate alternate site on temporary basis Internet Service Provider to be contacted for providing WAN connectivity from alternate site; limited connectivity with link to Disaster Recovery site. Inform employees to start working until normalcy is restored.

11. Network Diagram of Smc Insurance Brokers Private Limited's Office and Data Centre.

12. Non- Compliance

Failure to comply with this policy may, at the full discretion of M/s SMC Insurance Broking Pvt. Ltd., result in disciplinary action as per the policy.

End of Document