JK INSURANCE BROKERS

WE ARE ALWAYS THERE

Table of Contents

JK INSURANCE BROKERS LTD. NOIDA

1 PURPOSE

JKBIL's ability to continue operating as a viable business entity depends on having proper contingency plans and procedures in place. If a business disruption occurs, JKBIL must be able to resume operations in a reasonable time frame without compromising security.

This policy defines JKBIL's desired disaster recovery practice to ensure adequate mitigation of risks from interruption of Information Technology services.

2 SCOPE

This policy shall apply to all office locations and systems through which JKBIL's information assets are stored or processed, and all communication and network connections through which JKBIL's information assets are transmitted.

Technology systems, communications and network connections include, but are not limited to, network devices such as routers and firewalls, servers and mainframes, all operating systems, databases and applications.

3 POLICY

All JKBIL's information systems and assets shall be protected against potential failure or disruption of service through a formal business continuity plan and disaster recovery plan that:

- Restores assets in accordance with system or asset criticality to JKBIL business processes
- Maintains the required level of security over JKBIL's information assets in the event of a disruption. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

4 IT Availability Management

4.1 Capacity monitoring and planning

JKBIL shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of JKBIL.

4.2 System acceptance

Acceptance criteria for new information systems, upgrades and new versions shall include their ability to be resistant to disruptions or faults through appropriate design and

configuration and suitable tests to determine such capability shall be carried out prior to acceptance.

Where resistance to disruptions is not provided for through appropriate design and configuration, alternative mechanisms to provide for resistance to disruptions shall be evaluated for feasibility and implemented where feasible.

5 IT Continuity Management

5.1 Data backup

All data shall be backed up on a regular basis as per the Backup and recovery policy and the backups must be available for timely restoration in the event of information loss or disruption to ensure continuity of JKBIL's operations. The DR environment shall be kept in sync with the production environment at all times. All changes being applied to the production environment shall be applied to the DR environment as well to ensure the environments are in sync.

5.2 IT Continuity planning

An IT Continuity plan or disaster recovery plan shall be developed for each JKBIL or system based on appropriate risk assessment and business requirements and shall be approved by the ISRMC.

6 BCM Framework

JKBIL's BCM framework shall consist of documented business continuity and disaster recovery plans. A single framework shall be maintained to ensure all plans, across businesses and processes are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. The BCP/DR plans shall address at a minimum:

- Enterprise-wide business continuation
- Continuation of critical applications
- JKBIL's Data Center Disaster Recovery Plans
- Network connection / link
- Roles and responsibilities of all individuals in the Business Continuity and Disaster Recovery Plans

I. Business Impact Analysis

- RTO and RPO shall be defined for all applications based on the business requirements.
- All dependencies on IT systems by the business functions shall be clearly documented.

II. Risk Management and Evaluation

- JKBIL shall ensure that adequate coverage is provided in the identification of threat that may cause disruption to the availability of the IT assets supporting the business operations.
- A defined and documented Risk Assessment Methodology shall be used to conduct the Risk Assessment Exercise.
- Risk Analysis shall be performed at least on an annual basis.
- The acceptable levels of risk shall be defined, documented and approved by the management.
- Existing controls shall be assessed for their strength and effectiveness. The mitigation of a risk due to the presence of existing controls shall factor in the control strength and control effectiveness values.
- Control assessment may be undertaken on a sampling basis as required. In such cases, the sampling frequency shall be clearly documented.
- All risks having a risk rating above the acceptable level of risk shall have risk mitigation plans. These plans shall be approved by the management.
- Risk Mitigation plans shall have clearly defined ownership for the action points.
- The Risk Mitigation plan shall be reviewed and tracked to closure on a quarterly basis.

III. IT DR Strategies

- The IT DR strategy must ensure minimal data loss during exigencies and enable quick recovery and continuity of critical business operations.
- The strategies chosen shall be capable of supporting and integration with the business continuity of JKBIL.
- Strategic options shall be evaluated for the technology components and appropriate strategies shall be defined for recovery and restoration of IT systems as per recovery priority.
- External (third party) products and services shall be covered by the strategic options chosen where appropriate.
- To prevent the synchronization issue among inter-related applications during disaster, the IT DR plan shall include continuous operation-data mirroring to offsite location and stand-by computing and telecommunication

IV. IT DR Recovery Planning

- The response and recovery plan shall be concise and accessible to those responsible.
- The purpose and scope of each IT DR plan shall be defined, approved and understood.
- The plan shall set out prioritized objectives in terms of:
    - Critical IT services to be recovered.
    - Time span in which they are recovered.
    - The situation for invoking plans.

JK INSURANCE BROKERS NOIDA

- The recovery levels for each critical IT service.

- The IT DR Plan shall ensure that configuration of servers, network devices and other products at the DC and DR are identical at all times.
- The IT DR plan shall include periodic checks with reference to ensuring data and transaction integrity between DC and DR.
- The IT DR plan shall ensure that support infrastructures at DC and DR have no single point of failure and building management and monitoring systems are present to constantly and continuously monitor the resources.
- The data replication mechanism to be followed in IT DR plan shall ensure RPO compliance for critical applications.
- Stages of escalation and trigger events (interruption, single point of failure) shall be clearly defined.
- Specific IT DR Plans shall be documented and approved for each application. IT DR shall provide detailed instructions on the recovery and restoration of IT processes and systems for each application.
- Technology Recovery Procedures for recovering the IT services shall be developed and coverage shall be given to the following areas:
  - Detailed procedures to restore the application, databases and the associated hardware at the alternate location, taking into account the changed environment.
  - Detailed procedures to restore the network accessibility
  - Procedures for data synchronization and handling of the backlog of information resulting from the disruption.
- Changes required from the end user to access the application.
- IT DR plans shall be reviewed at least on an annual basis.

V. Training and Awareness

- A formal training program comprising of targeted courses and awareness sessions for the relevant staff shall be developed.
- A process shall be established for evaluating the training requirements for the staff identified to play a key role in the recovery of the IT systems. Appropriate training programs shall be conducted based on the level of skillset and proficiency determined to enable the person to perform the task.
- DR Drill shall be performed to ensure adherence to Business Continuity metrics.
- Alternative site options and resource availability shall be planned as a part of Business Continuity and tested for the same.
- Periodic Participation of JKBIL in national/ sectoral/ Organisational Cyber Security Exercises.

6.1 Outsourced relationship management

All information and applications outsourced to a third-party service provider shall include adequate plans for continuity of service developed and tested by the third-party service provider and approved by JKBIL. An JKBIL liaison with the third-party service provider shall

supervise execution of the disaster recovery activities in the event of a disruption of service to the JKBIL.

6.2 IS consideration in BCM

- A managed process shall be developed and maintained for business continuity throughout the JKBIL that addresses the information security requirements needed for the JKBIL's business continuity.
- A comprehensive Business Continuity Plan (BCP) shall be developed and implemented in order to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The BCP shall include effective Disaster Recovery procedures for quickly recovering from an emergency with minimum impact to the company's operations.
- Business Continuity Plan shall be developed based on critical business processes and the likely disruptive events along with their probability, impact and consequences for information security identified through Business Impact Analysis.
- It shall be ensured that any new application introduced in the IT environment of JKBIL shall have a documented ITDR processes based on its criticality and shall integrate with the existing recovery processes. It shall also have a business defined RTO and RPO.
- Any changes made that may have an impact on the developed recovery procedures shall be duly identified as a part of the change control process and shall be approved by the ITDR Manager before implementation.

6.3 Testing of BCP

- The business continuity and DR plans shall be tested at least once annually or when significantly changed to identify incorrect assumptions, oversights, or changes in equipment or personnel.
- Test results shall be reported to the ISRMC and shall be used to revise the BCP / DRP
- IT DR testing framework shall include DR drills that represent not only plan shutdown but also real disaster scenarios.
- All IT DR tests shall be conducted after careful planning to ensure no disruption to the business operations. All risk factors shall be documented and communicated to all affected persons prior to test.

6.4 Review of BCP

BCP shall be reviewed as per periodicity defined in the BCP itself and after each test and updated to ensure that the BCP considers the effectiveness of the current nature of business processes, infrastructure, personnel, etc

JK INSURANCE BROKERS LTD. NOIDA

7 Roles & Responsibility Matrix (RACI)

Responsible	Accountable	Consulted	Informed
IT	IS	Risk	Business users

8 Compliance

All users must comply with our company's corporate policies. Any user found to be abusing the privilege of using our corporate assets and access to business systems, or not in compliance with any of these policies, may be subject to disciplinary action, up to and including termination of employment.

9 Disciplinary Process

At JKBIL, we have established a disciplinary action policy to ensure a productive and respectful work environment. The following disciplinary measures may be implemented when employees fail to meet the expected standards of conduct and performance:

- Counselling
- Written warning
- Salary deduction
- Termination with/without notice
- Termination of contract with/without notice (as the case may be)

For detailed information regarding disciplinary action, please refer to Annexure A.

10 Applicability

This policy is applicable to all company employees/contractors working both on site and remotely.

JK INSURANCE BROKERS LTD NOIDA