

 InsightSCS	COMPANY POLICY Insight Supply Chain Solutions Corp.	Doc. No. 2019ISCSOPS-001	
		Version:	1.0
Department: Operations		Effective:	01 January 2019
Subject: Business Continuity Management Policy			

BUSINESS CONTINUITY MANAGEMENT POLICY

1. Policy Statement

To meet the enterprise business objectives and ensure continuity of its operations, InsightSCS Corp. shall adopt and follow well-defined and time-tested plans and procedures, build redundancy in teams and infrastructure, and manage a quick and efficient transition to the backup arrangement for business systems and services. Business Continuity Management (BCM) Policy reiterates the commitment of InsightSCS Corp. towards delivering the fastest transition and the highest quality of services through backup arrangement ensuring that the customers, business activities and services do not suffer in any way. The Business Continuity Management Procedure, Backup Policy and Backup Procedure shall be referred. The plan shall be available to Executive Leadership Team and Business Continuity Management team members of InsightSCS Corp.

2 Purpose

The main objective of Business Continuity Management is to minimize/eliminate the loss to an organization's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction. The Business Continuity Policy intends to:

- Establish a systematic approach for business continuity
- Create awareness amongst the concerned employees, about the business continuity aspects of InsightSCS and its importance.
- Test and review the business continuity plan for the organization.

3 Scope

3.1 IT Assets

BCM covers all IT assets and applications for a business transaction that are owned or utilized by InsightSCS Corp. See Appendix A. Disaster Recovery Summary.

3.2 Documentation

The BCM documentation shall consist of Plans and Resumption procedures for each service.

3.3 Document Control

The BCM document and all other referenced documents shall be controlled. The version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

3.4 Records

Records being generated as part of the BCM shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.



COMPANY POLICY
Insight Supply Chain Solutions
Corp.

Doc. No. 2019ISCSOPS-001

Version: 1.0

Effective: 01 January 2019

Department: Operations

Subject: Business Continuity Management Policy

3.5 Distribution and Maintenance

The BCM document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the BCP document will be with the BCM team.

4 Privacy

The BCM document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

5 Responsibility

Role of BCM Leader shall be performed by BCM Team and include the following:

- a. Coordinate the development and maintenance of the Organizational BCM policy manual and get approval from management.
- b. Identify and declare disaster-scenarios according to the gravity of the disaster.
- c. Enforce BCM among teams as per disaster scenarios.
- d. Review and audit BCM Policy at planned intervals.
- e. Test and update Business Continuity Plan at planned intervals.
- f. Facilitate functional training of the members for BCM execution.
- g. Co-ordinate with outsourcing partners wherever applicable.

Following are the primary roles of BCM Team Members:

- a. Execute BCM activities as per respective procedures.
- b. Co-ordinate with outsourcing partners wherever applicable.

6 Policy

- a. For catastrophic and major disasters, the BCM Leader shall invoke the BCM process in consultation with the BCM Team Members.
- b. It is the responsibility of the BCM Leader to ensure that adequate spare resources are available for recovering from a disaster in the infrastructure level.
- c. It is mandatory for all BCM Team Leaders to maintain the BCM document in an easily accessible and secure location.
- d. The BCM Policy shall be updated whenever major additions, upgrades, deletions take place to the underlying hardware, network environment, office infrastructure or key personnel.
- e. The BCM Policy and Plan testing process for vital services shall be done at least once in a year.

7 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.



Appendix A.

DISASTER RECOVERY

You

11



Business Continuity Plan Summary

1. Web Apps are hosted by Digital Ocean.
2. Digital Ocean has 8 datacenters around the globe.
3. Digital Ocean's Disaster Recovery (DR) & Security protocols are built-in.
4. Daily backups of DB at 3 am.
5. Weekly snapshots of deployed web Apps and critical directories.
6. Transactional processing - in case of a total disaster situation, we can go back to the last good/recovered transaction and re-process the transaction to full restoration.

INTERNAL AND PRODUCT DESIGN USE ONLY. DO NOT DISTRIBUTE.