IRIS BUSINESS SERVICES LIMITED



Business Continuity Plan

Version 1.5

Mar-2023

This document contains sensitive & confidential information, and should not be disclosed, transmitted, duplicated, used in whole or part other than for its intended purpose and intended recipients.

Document Information

Document Name	IBSL – Business Continuity Plan	**Version :**	1.5
Date Created	28 August 2017	**Released Date:** 9th Mar 2023	
Document No. : ISMS 14 **Classification :** Internal			

Prepared By	Information Security Team	**Document Owner**	Head-IT (CTO)
Reviewed and Approved By	(CIO/CTO)	**P K X Thomas**	P K X Thomas

Distribution: To all employees and relevant consultants, contractors, vendors and third parties of the IRIS Business Services Limited (IBSL).

Review history:

Sr.No.	Author	Date	Review details	Version Number
1	CISO	28th August 2017	Initial Release	Ver 1.0
2	CISO	21st September 2020	Annual Review	Ver 1.2
3	CISO	21st September 2021	Annual Review	Ver 1.3
4	CTO	18th August 2022	Annual Review	Ver 1.4
5	CTO	9th March 2023	Annual Review	Ver 1.5

Summary of changes from the previous release

Sr. No.	Version	Brief Description of the change(s) made
1	1.0	Initial release
2	1.1	Change in team members
3	1.2	Changes according to change in scope from product specific to enterprise level certification ● Replaced IRIS GST Reference with IBSL, organization as a whole ● Change in CMT Team Members in Appendix 'B' - Replaced Rohit Jha with Nishant Kumar
4	1.3	Added pandemic – related controls Updated team members Updated Non-availability of Building & Furniture
5	1.4	Annual Review

		• Change in CMT Team Members in Appendix 'B' - Replaced Rajendra Patil with P K X Thomas • Change in CMT Team Members in Appendix 'D' - Replaced Rajendra Patil with Sabu O
6	1.5	• Change in Appendix 'D': BCMT Member List • Change in Server Administrators in Appendix 'F' - Replaced Sabu O with Mahesh Tilave

Table of Contents

1. INTRODUCTION 5
2. OVERVIEW OF BCP 5
2.1 OBJECTIVE 5
2.2 SCOPE 6
2.3 ASSUMPTIONS 6
2.4 DEVELOPMENT 6
3. TESTING STRATEGY 7
3.1 GENERAL APPROACH TO TESTING 7
3.2 FREQUENCY OF BCP TESTS 7
3.3 ESTABLISHMENT AND EVALUATION OF BCP TEST SUCCESS 7
3.4 MAINTENANCE 7
3.5 CRISIS MANAGEMENT TEAM STRUCTURE 7
4. BCP OPERATIONAL INFORMATION 8
4.1 BCMT – BUSINESS CONTINUITY MANAGEMENT TEAM 8
4.2 BCMT TEAM STRUCTURE 8
4.3 IT SYSTEMS ENGINEERS 8
4.4 SERVER ADMINISTRATOR(S) 8
4.5 PROJECT MANAGER 8
4.6 CISO 8
4.7 OPERATING ENVIRONMENT AND RECOVERY PROCEDURE 9
4.8 IBSL OPERATIONS 9
4.9 BUSINESS CRITICAL ASSETS 9
4.10 CRITICAL DEPENDENCIES 9
4.11 IT SYSTEMS ENGINEERS 9

4.12 SYSTEM PROCEDURES 9
4.13 RECOVERY PROCEDURES 10
4.14 SUPPORT DEPARTMENTS 10
5. PREVENTIVE MAINTENANCE 10
5.1 PM'S ROLE 10
5.2 BCMT MANAGER ROLES 10
5.3 BCP EXERCISE AND DRILLS 11
5.4 INTER GROUP TRAINING 11
5.5 EMERGENCY OPERATING ENVIRONMENT 11
6. INFORMATION SECURITY RISK ASSESSMENT 11
7. RESULTANT SCENARIOS 11
7.1 MINOR BREAKDOWN 12
7.2 MAJOR BREAKDOWN 12
7.3 NON-AVAILABILITY OF BUILDING & FURNITURE 12
7.4 NON-AVAILABILITY OF RESOURCES 12
7.5 NON-AVAILABILITY OF SERVERS 13
7.6 NON-AVAILABILITY OF COMMUNICATION OR DATA LINK 13
APPENDIX – A: CRITICAL RESOURCES FOR BCP 14
APPENDIX 'B' CMT TEAM MEMBERS 15
APPENDIX C: DECISION FOR INVOKING THE BCP 16
APPENDIX 'D': BCMT MEMBER LIST 17
APPENDIX 'E': IT SYSTEMS ENGINEERS 17
APPENDIX 'F': SERVER ADMINISTRATORS 17

BUSINESS CONTINUITY PLAN

1. Introduction

This plan focuses on sustaining critical business operations of IRIS Business Services Limited (IBSL) during and after business disruption. This plan refers to a coordinated strategy involving plan, procedures and technical measures that enable the recovery of process after disruption.

Preparation for, response to, and recovery from a disaster affecting the IBSL operations requires the cooperative efforts of many recovery teams comprising of members from support groups and the functional areas supporting the operations. This document records the Plan that outlines and coordinates the efforts of various recovery teams.

For use in the event of a disaster, this document identifies the recovery facilities (Alternate sites) that have been designated as backups if the primary functional areas are disabled and critical business processes need to be accommodated in the recovery facilities.
This document identifies the Crisis Management Team, Information Security Department and other recovery teams along with their Roles & Responsibilities.

2. Overview of BCP

2.1 Objective

The purpose of the Business Continuity Plan is to provide an effective documented framework and a process to manage critical IT activities & their dependencies in case of an emergency.
The objectives of the Business Continuity Plan are:

- To mitigate the possible impact of an interruption to the activities
- To ensure security of information or data during disaster and
- To recover processes at identified recovery facilities & to meet the Recovery Time of 6 hours

This Business Continuity Plan specifies the responsibilities of the Crisis Management Team (CMT), the CISO, IT Head/VP and the Business Continuity Management Team (BCMT) with a common mission of establishing procedures to ensure the continuity of the operations in case of disaster.

- Note - IBSL is one of the core software product developed by IBSL and the software development server of which is hosted by Amazon Web Services (AWS). AWS maintains a “high availability” of server environment which means in the event of disaster, the data and application will be seamlessly available on parallel server located at different site of AWS. With this, the IBSL local team is left only with maintaining the BCP of support services and IBSL user’s peripheral facilities.

2.2 Scope

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of IBSL's IT Data Center as well as supporting facilities. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document. This plan focuses on the recovery of technology facilities and platforms, such as critical applications, databases, servers or other required technology infrastructure. Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

The scope of this plan is focused on disasters such as fires, floods, pandemics, epidemics and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters such as war, or nuclear holocaust. However, it can provide some guidance in the event of such a large-scale disaster.

2.3 Assumptions

The following assumptions are made in the Business Continuity Plan:

- Key personnel and/or their backups identified in the plan are available.
- Recovery location(s) and facilities as required are available that can handle the specified recovery activities.
- BCP shall not apply to non-recoverable situations such as countrywide disaster.
- BCP shall not be invoked for addressing day-to-day failures like link or system failure.
- The acceptable downtime is 6 hours after which the BCP will be invoked.

2.4 Development

The Executive management and Steering committee will constitute a Crisis Management Team (CMT) consisting of senior management, CISO and Project manager. The CMT members will constitute and develop the BCMT consisting of resources required for the continuity of business operations.

The BCMT will consist of technical and non-technical employees required for the recovery of systems, client services and management purposes. During the crisis, CMT members will oversee and ensure that the BCMT follows the process for recovery defined in the BCP for business continuity plan. Information Security Department head/CISO will develop the BCP organization and functional structure as per inputs provided by the Project manager, Department Heads and the Management. The current BCP covers the information resources defined in the Appendix –A: Critical Information Resources.

- RTO - The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster. In case of IBSL and support services, the RTO is defined as 06 hours.

- RPO - Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold. In case of IBSL and support services, the RPO is defined as 24 hours.

3. Testing Strategy

3.1 General Approach to Testing

The Testing Strategy identifies the actions to be taken to ensure periodic testing of BCP and DR plans, appropriate management review of all findings and the timely correction of any identified deficiencies.

3.2 Frequency of BCP tests

Plans must be tested at least once in every twelve-month period.

3.3 Establishment and evaluation of BCP test success

The test does not need to invoke all components of the plan concurrently. If the linkages among components have been sufficiently established and tested, testing may be conducted at a component level. Records of BCP test shall be maintained.

3.4 Maintenance

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the updated Plan; and training personnel. The ISD head/CISO is responsible for this comprehensive maintenance task while the CMT members will provide their inputs for any major business changes that could impact the BCP.

3.5 Crisis Management Team Structure

The CMT team consists of management people with varied roles. The key members are: CEO, Directors, IT Head / VP, CISO, Information Security Department and Project manager.

Refer To appendix ‘B’ for the details of the CMT team members. The CMT team member is authorized by the Executive board and ISD to invoke the BCP. The CMT team members will evaluate the disastrous situation based on the parameters defined in Appendix “C” before invoking the BCP. In case for what so ever reason none of the CMT team members is contactable, the BCMT manager can take a decision based on the parameters defined in the Appendix “C”.

4. BCP Operational Information

4.1 BCMT – Business Continuity Management Team

BCMT team consists of BCMT managers and employees, who will work on the recovery site to setup the systems, use the systems to deliver services and information to the clients. At least one BCMT team shall be constituted per location. BCMT managers will also check for any resource changes in the team on monthly basis.

4.2 BCMT Team Structure

BCMT team consists of employees from various functional departments as mentioned below. The BCMT Organizational Chart has been placed at Appendix 'D'.

4.3 IT Systems Engineers

IT Service Engineers will help in installation of the required software's and restoring backups on the desktops. Refer to Appendix 'E' For the IT Systems Engineers names.

4.4 Server Administrator(s)

Server Administrators will reinstall the servers and restore backups so that the server side services could be restored.

4.5 Project Manager

Project Manager of IBSL will co-ordinate with the team members internally and the clients externally during a disaster so that client can be kept informed about the state of recovery process and the operational services. Project Manager also participate in identifying and prioritizing the tasks for the smooth recovery of the operations.

4.6 CISO

CISO will create the BCP based on the inputs provided by the IBSL Project Manager, Department Heads of Associated Support Services and the management. The CISO will discuss the recovery parameters and the critical information resources with the PM/Department Heads and accordingly formulate a BCP. The PM's, Department Heads and the management people will provide the details of the critical resources and the manpower required for recovery of the operations. CISO will also recommend the technological requirements for the BCP. CISO will chalk out a comprehensive recovery plan and submit to the Steering Committee for implementation approval.

4.7 Operating Environment and Recovery Procedure

IBSL has number of business units each one having its own processes and procedures. Some departments are critical as they process information related to client. Only these units have been considered for the BCP.

The details are as listed below –

- Product Development Team (Source Code, Patches),
- Human Resource (Employee Records)
- IT Infrastructure (Mailing Service, Active Directory, File Servers)
- Legal & Finance (Legal Contracts, Financial Data)

4.8 IBSL Operations

IBSL is a global provider of structured data solutions that help entities create, collect & consume business & financial data

4.9 Business Critical Assets

As Identified by PM are listed in Asset Inventory project wise.

4.10 Critical Dependencies

a. Data Center at Amazon Web Services, Azure, Data Center at BKC and on premise at Vashi Office
b. Internet Bandwidth
c. Development Softwares: Java, Open Project, GitLab, .Net, PHP, Pyhton ,TFS, Quick Scrum

4.11 IT Systems Engineers

Supporting IT infrastructure: Workstations (Desktops/Laptops), Network (LAN & Switches), Firewall and Router, Uninterrupted Power Supply (UPS)

4.12 System Procedures

Mail services are migrated to GMail, maintained by Google. Backups are maintained on cloud by Google.

4.13 Recovery Procedures

AWS/Azure maintains high availability of data center services for IBSL, which means, parallel set of servers are running with real time data replication. This enables server switching on real time basis without any interruption and zero downtime.

Leased line internet links available to provide internet connectivity with uptime commitment of 99%. The leased line links terminate on the hardware firewall installed in server room and users can be connected with high speed internet connection. High Speed data cards have been allocated to the Team Leaders for data upload and delivery in case of emergency situations such failure of leased line.

Power backup is taken care by the Emerson 40kVA ups installed at the Vashi

4.14 Support Departments

Critical data of associated support departments i.e. Technology, Finance, HR & Admin is being backup on regular basis.

At Vashi a NAS storage device has been installed for taking backups. Source code backup is done on weekly basis by ITSS team.

HR-Admin is currently using ESSL software; backup of data on ESSL is on regular basis by ITSS team.

Accounts department has installed one separate Tally server which holds all the data. The backups of Tally server are also taken on weekly basis.

5. Preventive Maintenance

5.1 PM's Role

PMs are responsible for following activities:

- Maintenance of personnel skill matrix
- Updating needs for changes in BCP plan to CISO

5.2 BCMT Manager Roles

BCMT managers are responsible for:

- Maintaining an updated list of resources along with their contact numbers and email ID's.
- Practice of BCP drill (BCP testing Plan)
- Inter group training for cross functional tasking
- Taking decision to invoke the BCP in case CMT members are not available.

5.3 BCP Exercise and Drills

It is intended to carry out BCP exercises in future so that scenario of all possible disasters could be simulated. The planning of all exercises would also depend upon the inputs by Project manager and the client requirements. The CISO will evaluate the technologies and recommend solutions for the BCP implementation and will present the same to the Steering Committee for approval.

5.4 Inter Group Training

An effort is in hand to identify resources from other Departments, who could be trained on the functional aspects of organization. Project manager and Department heads have been requested to nominate resources who could be spared in case of an outage due to disaster. These resources will be imparted training on a high level related to various functionalities of IBSL business operations.

5.5 Emergency Operating Environment

To create an environment for facilitating all business operations during outage of a disaster, we need to understand the impact of various disasters. This would help in creating an environment suitable for the smooth business operations and continuity of all business-related deliveries. The Emergency Operating Environment has been carefully considered based on the impact of various possible disasters.

The table in Appendix –'C' depicts the impact of various possible disasters.

6. Information Security Risk Assessment

Business impact analysis or the risk assessment should be carried out from Information Security Point of View for all Critical Information Assets

Refer 'IBSL - Risk Assessment & Mitigation Plan'

7. Resultant Scenarios

The resultant scenario of above mentioned impacts could be classified in terms of minor and major breakdowns. The minor breakdowns can mostly be taken care of by ITSS Department, Operations and the Administration and they may not involve any relocation of the resources. ITSS Department, Operations and the Administration would also take care of major breakdowns but they would also require an active participation of the Groups being affected. A major breakdown may or may not call for the relocation of resources. The possible reasons for these breakdowns and their associated recovery plans are discussed in the succeeding paragraphs.

7.1 Minor Breakdown

Affected Teams are unlikely to perform business operations for a short duration of time (less than 4 hours) for all projects. Minor breakdowns may be caused by power failure, Virus attack, non-availability of air-conditioning, breakdown of servers, malfunction of individual workstations, temporary network disruption, minor fire and data link failures etc. These breakdowns generally do not affect the business operations. System recovery Procedure as already discussed can be followed for the recovery process. While restoration of power, minor fire and air-conditioning will be taken care of by administration, restoration of network, workstations and data link will be handled by ITSS operations.

7.2 Major Breakdown

If business operations of the organizations are affected due to any of the disasters and the restoration process may take longer time (more than a day). Under these circumstances, the recovery plan would depend upon the outage of disaster, taking into account its volume and gravity.

The BCMT will handle these outages as follows:

7.3 Non-availability of Building & Furniture

In case the existing premise is not available for working, IBSL team can connect to Gitlab or AWS environment from their homes also. Since Gitlab and AWS are connected through internet and Active Directory authentication is not required, user can resume working from any location. Carbon & eAudit are hosted on Azure with uptime commitment. iFile & iDeal are on client premise and for which BCP process is followed.

IBSL team can also work remotely, if and when the need arises, using VPN to connect to the IBSL network and access any confidential data securely. VPN licenses have been procured in such a fashion that 100% of the taskforce are able to work remotely provided that a stable internet connection is available at the remote location from where the employee plans to work.

7.4 Non-availability of Resources

Non-availability of resources could be partial or total and this could be the result of any of the following reasons:

- Total disruption of traffic due to heavy storm/rain/flooding
- Political band leading to non-availability of transports
- Railway/Transporter’s strike
- Accident while at work
- Pandemics or Epidemics

The ITSS head will liaise with HR-Administration for alternate means of transportation of its resources in case the conventional mobility is not likely to be restored within a day or two.

The resources will be contacted telephonically (land line / cellular phones) and they will be advised to assemble at pre-defined pick-up points. Cross trained resources may be inducted from other departments on temporary basis to make up for the shortfall of resources.

7.5 Non-availability of Servers

AWS/Azure maintains high availability as server redundancy is also provisioned in the existing service package

- Non-availability of Work Stations

If workstations of the individual users get damaged, ITSS team is expected to have arrangements to hire or procure the workstations at short notice so that ITSS resources could continue to work at the existing location. If the business units along with the furniture and ITSS infrastructure get damaged, all efforts will be made to accommodate the ITSS resources at any of the alternate offices subject to availability of workstations. In case of an inescapable situation, resources may be issued data cards and laptops and allowed to work from home until the site is restored.

7.6 Non-availability of Communication or Data Link

Vashi office should have two internet connections are described in the table:

Sr.no	Office Location	Primary Link	Secondary Link
1.	Vashi	STPI leased line 60 MBps	I-One 50 MBps

APPENDIX – A: Critical Resources for BCP

Information Resource	Department	Location	Availability required
Core Business Applications	IBSL	Vashi	Software Dev Environment
ESSL	HR	Vashi	Attendance Record
Tally	Finance	Vashi	Accounting Record

Appendix 'B' CMT Team Members

Sr.no	Name	Email ID	Contact Number
1	P K X Thomas	pkx.thomas@irisbusiness.com	98672 47606
2	Deepta Rangarajan	deepta.rangarajan@irisbusiness.com	9594031317
3	K.Balachandran	k.balachandran@irisbusiness.com	9821231314
4	Shailesh Gupta	shailesh.gupta@irisbusiness.com	9810766773

Appendix C: Decision for Invoking the BCP

Sr. No.	Disaster	Building+ Furniture	Human Resources	Hardware	Software	Communication Lines
1	Fire	✓	✓	✓	✓	✓
2	Natural calamities /manmade disasters	✓	✓	✓	✓	✓
3	Non Availability of Employees		✓			
4	Hardware Break-down			✓		✓
5	Virus attack or Hacking				✓	
6	Telecom / Internet link failure				✓	✓
7	Power failure			✓		✓
8	AC Failure			✓		✓

Appendix 'D': BCMT Member List

Sr.no	Location	Name	Role
1.	Vashi	Mahesh Tilave	BCMT Manager
2.	Vashi	Vikas Mithbawkar	BCMT Manager

Appendix 'E': IT Systems Engineers

Sr.no	Location	Name	Contact No.
1	Vashi	Rajit Sahu	9930008082
2.	Vashi	Ramesh Kone	9619197547

Appendix 'F': Server Administrators

Sr.no	Location	Name	Contact No.
1.	Vashi	Vishal Vare	9969274106
2.	Vashi	Mahesh Tilave	9870791914