A.S.K. Services INTL
8th Floor, The Core, 62 ICT Avenue, Cybercity, Ebene 72201, Mauritius T: +230 489 9090

Disaster Recovery and Business Continuity Policy

MARCH 2025

8th Floor, The Core, 62 ICT Avenue, Cybercity, Ebene 72201, Mauritius T: +230 489 9090

Table of Contents

1. INTRODUCTION

Mandatory

This Disaster Recovery Plan (hereinafter referred to as the "DRP" and/ or the "Disaster Recovery Plan" and/ or the Policy) captures, in a single repository, all of the information that describes the Company's ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery.

This Policy defines acceptable methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services. The disaster recovery standards in this Policy provide a systematic approach for safeguarding the vital technology and data managed by the Information Technologies and Services Department. This Policy provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by A.S.K. Services INTL.

The purpose of the Business Continuity and Disaster Recovery Policy (the "**Policy**") is to outline the course of action for the continuation of critical business functions and the measures for recovery in the event of a disaster.

This Policy's main and immediate goals are to:

- provide an orderly and efficient transition from normal to emergency conditions;
- provide specific guidelines appropriate for complex and unpredictable occurrences;
- assure consistency in action throughout all levels of the Company and prevent activity inconsistent with the policies of the Company;
- establish a management succession and allocate emergency powers and authorities;
- provide a standard for testing the implementation of the Policy;
- safeguard the operation of the critical activities and return the same to the normal course of business;

provide rules on the implementation, functionality, and review of the Policy;

2. Definition of a Disaster

A disaster can be caused by man or nature and result the Company's department not being able to perform all or some of their regular roles and responsibilities for a period of time. The Company defines disasters as the following:

This Policy is implemented in order to minimize the impact of significant incidents on the Company's services and recover from the unavailability of IT systems to an acceptable level through a combination of responsive and recovery controls. To achieve this, the following three objectives are set out:

- Establish operational control of the disaster
- Communicate with relevant parties impacted by the disaster
- Activate a specific recovery plan in relation to the disaster

The following events can result in a disaster, requiring this Disaster Recovery Plan to be activated:

- Fire
- Flash flood
- Pandemic
- Power Outage
- War
- Theft
- Terrorist Attack

The purpose of this policy is twofold: first, to capture all of the information relevant to the enterprise's ability to withstand a disaster, and second to document the steps that the enterprise will follow if a disaster occurs.

Note that in the event of a disaster, the first priority of the Company is to prevent the loss of life. Before any secondary measures are undertaken, the Company will ensure that all employees, and any other individuals on the organization's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of the Company will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- Preventing the loss of the organization's resources such as hardware, data and physical IT assets
- Minimizing downtime related to IT
- Keeping the business running in the event of a disaster

This policy will also detail how this document is to be maintained and tested.

The Company's DRP takes all of the following areas into consideration:

- Network Infrastructure
- Servers Infrastructure
- Telephony System
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems
- IT Documentation

3. Premises

The Company's registered office is located at 8th Floor, The Core, 62 ICT Avenue, Cybercity, Ebene 72201, Mauritius.

The registered office has access to essential utilities for carrying out the activity in optimal conditions. Also, the security and protection of these offices is ensured with adequate security elements, while the physical office benefits from 24/24 surveillance and monitoring.

In the event that access to these premises is compromised for 48 hours or more, or if the utilities essential to the Company's operation are interrupted for more than 48 hours, the Company's activity will not be affected and will be able to continue as usual.

4. Data center, access to data and back-up

The Company server is stored in a cloud-based solution. The server can be accessed from the laptop only through a password protected VPN connection. The contents of the server are backed up daily.

The Company has a strict procedure of saving the documents on the server immediately after receiving

the same from our customers, suppliers, collaborators, employees, etc. The staff is trained and follows the procedure of saving the documents in the dedicated folders for each client, customers, suppliers, collaborators, employees, etc. and no documents will be saved elsewhere.

5. Confidentiality, security, and reliability of client information

Every staff and members of Management Team is subject to a duty of secrecy towards the Company. In accordance with this duty, no details of clients' dealings or positions or any other confidential or price-sensitive information may be either discussed or disclosed outside the premises of the Company, except with the specific written authorization of the Board of the Company or, in the event of a legal/regulatory requirement to disclose information. This provision is also included in the contract of employment for all employees.

6. Dealing with a Disaster

If a disaster occurs in the Company, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

1) Disaster identification and declaration
2) Communicating the disaster
3) Assessment of current and prevention of further damage
4) Standby facility activation
5) Establish IT operations
6) Repair and rebuilding of primary facility

7. Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, the Company must be prepared to find out about disasters from a variety of possible avenues. These can include:

- First hand observation
- System Alarms and Network Monitors
- Environmental and Security Alarms in the Primary Facility

- Security staff
- Facilities staff
- End users
- 3rd Party Vendors

8. Records

Electronic records, files and databases are needed to perform essential business processes, conduct key business operations while the Policy is activated, and to reconstitute normal operations after the event. All our records are stored in electronic form on our online server.

All documents and information received from our clients and information related to the administrative and organisational aspects of the Company are saved on the server following dedicated rules.

9. Disaster recovery measures

Depending on the circumstances of the disaster that occurred and based on the information at hand when the Policy has been activated, the Emergency Team will take the following measures:

(i) if the office premises become unavailable, staff will be instructed via e-mail to telework until further information becomes available; confirmation of receipt of the e-mail will be requested;

(ii) return to work will be scheduled and organised in groups;

(iii) if the disaster renders the access to the server unavailable, the IT Services Provider will re-establish the connection to the server in up to 30 minutes;

(iv) before returning to work on the office premises;

10. Restoring IT Functionality

Should a disaster actually occur, and the Company needs to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which the Company's information system will be recovered.

This section will contain all of the information needed for the organization to get back to its regular

functionality after a disaster has occurred.

11. Policy implementation

The person responsible for the implementation, maintenance and review of this Policy is the IT team.

The IT team will review the Policy, and the data associated with it (business impact analysis, risk assessment) at least once a year. Any changes of the content of this Policy or the data associated with it will be documented and attached to the Policy.

Each member of the Company's staff has been properly trained and informed about their role and responsibilities to assure the implementation of the Policy and the actions that are required on their behalf when the Policy is activated.

A copy of this Policy has been distributed to the staff at the beginning of the collaboration with the Company. A copy of this Policy is also available on the server in the dedicated folder, as well as on the Company's website.

The appropriate implementation of the Policy will be assessed at least once a year.