



FAWE LIBERIA IT DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

Acronyms and Abbreviations:

- BC – Business Continuity
- BCT - Business Continuity Team
- DR – Disaster Recovery
- DRP – Disaster Recovery Plan
- DRT – Disaster Recovery Team
- DR&BCP – Disaster Recovery & Business Continuity Plan
- ERT - Emergency Response Team
- FAWE Liberia – Forum for African Women Educationalists Liberia
- ICT – Information Communication and Technology
- ISP – Internet Service Provider
- RTO – Recovery Time Objectives

Table of Contents

• Acronyms and Abbreviations:	2
• Introduction:	4
• Objective:	5
• Scope:	5
• Assumptions:	5
• Custodian(s) of the Disaster Recovery Plan	6
• Changes to the disaster recovery plan	6
• Risk Assessment and Management	8
• Viruses/Malware:	10
• Disaster Recovery Team Activation	11
• Escalation Procedure	12
• Guidelines and situations necessitating the activation of the IT DR and BC Plan ..	12
• Backup strategy	13
• FAWE Liberia Security Levels:	14
DEPARTMENTS/UNITS AT FAWE LIBERIA AND ESSENTIAL TECHNOLOGICAL TOOLS OF TRADE	15
Revision History:	16

Introduction:

This IT Disaster Recovery & Business Continuity Plan is designed to ensure the continuation of vital business processes dependent on technology if a disaster occurs, providing an effective solution that can be used to recover all vital business processes within the required time frame. The IT disaster recovery plan is the cornerstone of an overall business continuity strategy which aims at maintaining a minimum level of service disruption while restoring **FAWE Liberia**'s operations to business as usual.

This document summarizes the minimum recommended procedures; however, in the event of an actual emergency, modifications to this document may be made to ensure physical safety of staff, systems and data.

This plan should be periodically tested in a simulated environment to ensure that it can be implemented in real emergency situations and that the management and staff understand how it is to be executed. The plan should also be kept up to date to consider the changing circumstances. It is prudent that the update process of DR&BCP is well structured and controlled. Whenever changes are made to this document, they should be fully tested.

Objective:

The overarching objective of **FAWE Liberia**'s disaster recovery plan is to develop, test and document a well-structured and easily understood plan that will help **FAWE Liberia** recover as quickly and efficiently as possible from an unforeseen disaster and/or emergency which interrupts and/or disrupts systems and normal ICT operations.

- To properly constitute a business continuity team that serves as liaison between the functional area(s) affected and service providers offering major services such as internet, telephony etc.
- To ensure employee safety as well as fully understanding their roles in the implementation of the DR & BC plan.
- To ensure the proposed contingency measures are efficient and cost effective.

Scope:

The scope of this business continuity and disaster recovery plan is limited to disruption in activities leading to the unavailability of FAWE Liberia's facilities and/or services that support the day-to-day functioning of the organization. The Business Continuity Plan includes procedures for all phases of recovery as defined within sections of this document.

Disaster Recovery shall focus on the recovery of technology facilities and platforms, such as critical applications, databases, servers, or other required technology infrastructure.

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

Assumptions:

The viability of this Business Continuity Plan is based on the following assumptions:

1. That a viable and tested IT Disaster Recovery Plan exists and will be put into operation to restore data center service at a backup site within five to seven days.

2. That the Organization's facilities management department has identified available space for relocation of departments which can be occupied and used normally within two to five days of a facilities emergency.
3. That this plan has been properly maintained and updated as required.
4. That each department has their own functional Business Continuity Plan.

Custodian(s) of the Disaster Recovery Plan

The DRP both in hard and soft copy shall be stored in a safe location as determined by the **FAWE Liberia** Management Team (MT)/Emergency Response Team (ERT)/Business Continuity Team (BCT). Copies of the same shall also be maintained off-site by each member of the management team. The disaster recovery team shall also maintain up-to-date copies of the DR plan which should be readily available in case of an actual disaster warranting the execution of the DR Plan.

Changes to the disaster recovery plan

Maintenance of the IT Business Continuity Plan within **FAWE Liberia** is the joint responsibility of the IT unit, HR unit, finance and administration and management.

IT unit shall be responsible for:

- Development and design of the IT DR/BC plan which includes identification of critical IT systems and data, assessing risks and defining the recovery objectives.
- Regular assessment of the IT infrastructure to identify vulnerabilities, assess hardware and software dependencies, and evaluate the readiness of backup systems and data centers.
- Implementation of appropriate backup solutions including testing and validation of the backups and backup systems.
- Documentation of detailed IT procedures for data and system recovery, ensuring that these procedures are well-documented, up-to-date, and readily accessible to relevant personnel as outlined in this document.

- Implementing monitoring systems to detect potential issues or disruptions that could lead to major service interruptions.

Evaluation and integration of cloud-based and off-site solutions for data storage and recovery.

Ensuring that communication channels i.e. email, and collaborations tools are quickly availed/restored during a disaster to facilitate communication among employees and stakeholders.

Maintaining relationships with vendors and suppliers to ensure the availability of necessary hardware, software, and services in case of equipment failure or damage during a disaster.

Participating in the regular review and update of the DR/BC plan to incorporate technological changes, system upgrades, and lessons learned from previous validation tests or incidents.

Initiating the IT-related aspects of the incident response plan when a disaster or disruption occurs. This includes coordinating recovery efforts, communication, and decision-making related to IT systems and data.

HR unit shall be responsible for:

- Ensuring that the plan aligns with the organization's human capital needs and that employees are prepared for their roles in disaster recovery and business continuity efforts.
- Collaborate with IT and other departments to identify essential roles and functions that must continue during a disaster, i.e., categorization of critical functions and ensuring adequate backup and succession plans are in place.
- Organizing and facilitating employee training for IT and Non-IT staff and awareness programs related to disaster recovery and business continuity. This includes educating employees about their roles and responsibilities in the event of a disaster.

Maintaining up-to-date employee contact information, including emergency contact details.

Ensuring that personnel policies and procedures are aligned with the DR and BC plan. This includes policies related to remote work, leave policies during disasters, employee safety etc.

Coordination and collaboration with external agencies, such as local authorities or emergency services, to ensure that employee safety and well-being are prioritized during a disaster.

Communication and notification efforts, such as informing employees about disaster preparedness measures, evacuation procedures, and updates during an ongoing disaster.

Finance and administration shall be responsible for:

- Resource allocation: ensuring the necessary budgetary resources for implementing and maintaining the IT DR/BC plan. This includes funding for equipment, software, training, and testing.
- Assessing the cost-effectiveness of various DR/BC strategies and solutions, helping to prioritize investments based on their impact on business continuity and risk mitigation.
- Overseeing insurance policies related to disaster recovery and business continuity as well as ensuring that the organization is adequately protected in case of a disaster.
- Maintaining financial records and documentation related to the IT DR/BC plan, including expenses, investments, and cost recovery procedures.
- Maintaining an inventory of critical IT assets and equipment required for disaster recovery and tracking of depreciation and replacement needs.
- Collaborating with IT to create annual budgets and financial forecasts for disaster recovery and business continuity efforts.
- Providing input and data for the business impact analysis (BIA) process, helping to identify financial risks, potential losses, and the financial impact of IT system disruptions.
- Ensuring participation in the business continuity exercises and training programs.

- Ensuring that financial and administrative policies and procedures are aligned with the IT DR/BC plan.

Management's responsibilities shall entail:

- Commitment to DR and BC planning through allocation of resources, including budget, personnel, training and creating a culture that values preparedness.
- Involvement in the risk assessment processes to identify potential IT-related disasters and their impact on the organization.
- Oversight on the development, maintenance, and testing of the DR and BC plan to ensure it aligns with organizational goals and regulatory requirements.
- Staff communication on the importance of the plan and providing necessary training and awareness programs.
- Supporting and participating in regular testing of the plan.
- Staying informed about legal and regulatory requirements related to DR and BC planning.
- Making critical decisions quickly, such as declaring a disaster and initiating the recovery process.
- Continuous improvement, i.e., reviewing incidents and lessons learned to enhance the plan continually.
- Institutionalizing proper reporting mechanism that aids in providing regular updates to the organization's stakeholders.

NOTE: The functions and roles referenced in this plan do not have to previously exist within FAWELiberia; they can be assigned to one or more individuals as new responsibilities or delegated to an external third party if funding for such services can be arranged and allocated.

Exceptions, Review, and Approval

- Exceptions: Written approval by Executive Director or Board.
- Review: Annually or on significant changes.

Review by:

Executive Director: _____

Hon. Millias Z. Sheriff

Date: _____

07/07/26

Approved by:

Chairperson, Board of Directors: _____

Atty. Evelyn F. Barry

Date: _____

07/07/2026



