BACKUP AND DISASTER RECOVERY POLICY

ITEC International Ltd (ITEC Ltd)
Tel +250 788620612
Email: info@itec.rw
Website: www.itec.rw
Rwanda

MARCH 2025

BACKUP AND DISASTER RECOVERY POLICY

1. **Purpose**

The purpose of this policy is to establish a framework for effective **data backup** and **disaster recovery (DR)** to ensure business continuity and minimize downtime or data loss in the event of a disaster or system failure.

2. **Scope**

This policy applies to:

- ✓ All employees, contractors, and IT personnel
- ✓ All critical systems, applications, and data under [Company Name] control
- ✓ Cloud-based and on-premises infrastructure

3. **Objectives**

- ✓ Ensure timely and complete backups of all critical data
- ✓ Enable rapid recovery of IT services following a disruption
- ✓ Maintain compliance with legal, regulatory, and contractual obligations
- ✓ Minimize business impact due to data loss or downtime

4. **Backup Policy**

4.1 Backup Frequency

- ✓ **Daily backups** for critical data and production systems
- ✓ **Weekly full backups** with daily incremental backups for non-critical systems
- ✓ **Real-time replication** for mission-critical databases (where feasible)

*4.2 **Backup Storage***

- ✓ Backups are stored in:
  - **Primary on-site servers**
  - **Secondary off-site or cloud-based storage** (e.g., AWS S3, Azure Blob, etc.)
- ✓ Backups must be encrypted in transit and at rest.

*4.3 **Retention Periods***

- ✓ Daily backups: Retained for **14 days**
- ✓ Weekly backups: Retained for **3 months**
- ✓ Monthly backups: Retained for **1 year**

4.4 Backup Testing

- ✓ Backup restoration tests must be conducted **quarterly**.
- ✓ Test results should be documented and reviewed by IT leadership.

5. **Disaster Recovery Policy**

5.1 Disaster Definition

A disaster is any unplanned event that causes significant disruption to IT services, such as:

- ✓ Cyberattacks (e.g., ransomware)
- ✓ Hardware or software failure
- ✓ Natural disasters (e.g., floods, earthquakes)
- ✓ Power outages or network failures

5.2 DR Objectives

- ✓ **RTO (Recovery Time Objective):** [e.g., 4 hours for critical systems]
- ✓ **RPO (Recovery Point Objective):** [e.g., 1 hour for critical systems]

5.3 Roles and Responsibilities

- ✓ **IT Manager:** Oversees recovery efforts and ensures adherence to the plan.
- ✓ **DR Coordinator:** Executes DR procedures and communicates with stakeholders.
- ✓ **All Staff:** Follow DR protocols and assist as needed.

5.4 Recovery Procedures

- ✓ Activate Disaster Recovery Plan (DRP)
- ✓ Assess damage and identify affected systems
- ✓ Restore services using prioritized recovery list
- ✓ Notify stakeholders and provide status updates
- ✓ Conduct post-incident review and update the plan accordingly

6. **Policy Compliance**

- Non-compliance may result in disciplinary action or increased business risk.
- Compliance is monitored by IT leadership and subject to audit.

7. Review and Maintenance

This policy and the DR plan must be reviewed **annually**, or after significant changes to infrastructure or business operations.

SIGNED BY ITEC LTD
Name: TWAGIRAMUNGU Serge
Title: Managing Director

Effective Date: April 30,2025
Review Date: April 30,2025