DATA BREACH RESPONSE PROCEDURE

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

MARCH 2025

1. **Purpose**

The purpose of this procedure is to provide a structured and effective response to any incident involving the unauthorized access, disclosure, loss, or destruction of personal data, in order to minimize risk and comply with legal and regulatory obligations.

2. **Scope**

This procedure applies to all employees, contractors, and third parties who handle or have access to the organization's personal data and information systems.

3. **Definition of a Data Breach**

A **data breach** is any incident that results in:

- Unauthorized access to personal data
- Accidental or unlawful destruction, loss, alteration, or disclosure of personal data
- Unavailability of data due to system failure or cyberattack

Examples include:

- Loss or theft of devices containing personal data
- Hacking or ransomware attacks
- Sending personal data to the wrong recipient
- Human error leading to exposure of data

4. **Roles and Responsibilities**

Role	Responsibility
Data Protection Officer (DPO)	Lead breach response, assess severity, report to authorities, and coordinate communication.
IT Department	Contain and investigate the technical cause of the breach, implement security measures.
Management	Approve decisions related to breach handling and notification.
All IT	Immediately report any suspected or actual data breach to the DPO or IT department.

5. **Data Breach Response Steps**

Step 1: Identification and Reporting

- Any employee who becomes aware of a potential or actual data breach must report it immediately to the DPO or IT Department.

- The report should include:
  - Date and time of detection
  - Description of the incident
  - Type of data involved
  - Number of individuals affected (if known)

Step 2: Containment

- The IT Department takes immediate action to isolate affected systems, stop unauthorized access, and prevent further data loss.
- Change passwords and disable compromised accounts if necessary.

Step 3: Assessment

- The DPO and IT team assess:
  - The type and sensitivity of data involved
  - Number of affected individuals
  - Potential harm or risk (e.g., identity theft, reputational damage)
  - Whether the breach is ongoing

Step 4: Notification

- **Internal Notification:** Management and key stakeholders are informed.
- **External Notification:**
  - If the breach poses a high risk to individuals, the DPO notifies the Data Protection Authority within **72 hours** (as required by GDPR or similar regulation).
  - Affected individuals are informed as soon as possible with clear guidance on how to protect themselves.

Step 5: Investigation and Documentation

- Conduct a detailed investigation to determine root causes and impacts.
- Document all findings, decisions, and actions taken.
- Maintain a **Data Breach Register** for audit and compliance purposes.

Step 6: Remediation and Prevention

- Implement corrective actions to prevent recurrence (e.g., stronger access controls, staff training, security updates).
- Review and update security policies as necessary.

6. **Communication Plan**

All public or media communications regarding the data breach will be managed by the Communications Office in coordination with the DPO to ensure accuracy and compliance with confidentiality obligations.

7. **Review and Testing**

This procedure shall be:

- Reviewed **annually** or after any major data breach
- Tested through **periodic simulations or tabletop exercises**

8. **Record Keeping**

All data breach reports, investigation records, and communication logs must be securely stored for at least **1 year** (or as required by applicable law).

9. **Policy Review**

This policy will be reviewed annually and updated as needed to align with evolving technologies and compliance requirements.

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

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