INCIDENT RESPONSE POLICY

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

MARCH 2025

INCIDENT RESPONSE POLICY

1. Purpose

The purpose of this Incident Response Policy is to establish a structured and effective approach for identifying, responding to, and recovering from cybersecurity incidents that threaten the confidentiality, integrity, or availability of ITEC Ltd's IT systems, data, or services.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and systems managed or owned by ITEC Ltd. It covers all types of security incidents, including but not limited to:

- ✓ Malware and ransomware infections
- ✓ Data breaches and data leaks
- ✓ Unauthorized access to systems or data
- ✓ Denial-of-service (DoS) or distributed DoS (DDoS) attacks
- ✓ Insider threats or policy violations
- ✓ Physical breaches affecting IT infrastructure

3. Definitions

- ✓ **Security Incident:** Any event that compromises the availability, integrity, or confidentiality of company data or IT assets.
- ✓ **Incident Response Team (IRT):** A designated group responsible for handling incidents and minimizing their impact.
- ✓ **Data Breach:** Unauthorized access, acquisition, or disclosure of sensitive or personal data.

---

4. Objectives

- ✓ Detect and confirm incidents quickly and accurately
- ✓ Contain and mitigate the effects of incidents
- ✓ Communicate effectively with stakeholders
- ✓ Investigate and document incident details
- ✓ Recover normal operations rapidly
- ✓ Prevent recurrence through root cause analysis and policy updates

5. Incident Response Roles and Responsibilities

Role	Responsibilities

Incident Response Team (IRT)	Coordinate response, lead investigations, and document findings.
IT Department	Provide technical support, implement containment measures, restore services.
Data Protection Officer (DPO)	Assess privacy impacts and ensure regulatory compliance.
Legal Team	Evaluate legal implications, manage external reporting and compliance.
Communications Team	Manage internal and external communication, including press releases if necessary.

6. Incident Response Lifecycle

ITEC Ltd follows a five-phase approach to incident response:

a. Preparation

- ✓ Maintain an up-to-date incident response plan.
- ✓ Conduct regular security awareness training for staff.
- ✓ Implement monitoring and alerting systems.

b. **Identification**

- ✓ Detect and validate security incidents using automated tools, reports, or user submissions.
- ✓ Record the time and method of detection.
- ✓ Notify the IRT immediately upon detection.

c. **Containment**

- ✓ Short-term containment: Isolate affected systems to prevent further spread.
- ✓ Long-term containment: Apply fixes, such as patching vulnerabilities or changing credentials.
- ✓ Maintain forensic evidence where needed.

d**. Eradication**

- ✓ Identify and remove the root cause (e.g., malware, unauthorized accounts).
- ✓ Strengthen affected systems and apply patches or upgrades.
- ✓ Validate that the threat has been removed.

e. **Recovery**

- ✓ Restore systems to normal operations from clean backups.
- ✓ Monitor systems closely for signs of reinfection or further issues.
- ✓ Document the timeline and actions taken.

7. **Reporting and Escalation**

- ✓ **Internal Reporting:** All employees must report suspected incidents immediately to the IRT or IT helpdesk.
- ✓ **Escalation Procedures:** Incidents are escalated based on severity levels (e.g., Low, Medium, High, Critical).
- ✓ **External Notification:** If personal data is involved, notify regulatory bodies (e.g., under GDPR, within 72 hours) and affected individuals as required.

8. **Communication Plan**

- ✓ Use a designated incident communication channel (e.g., secure email, Teams/Slack).
- ✓ Limit information sharing to authorized personnel only.
- ✓ Prepare official communication templates for internal updates, customer notifications, and regulatory disclosures.

9. **Documentation and Evidence**

- Maintain an incident log for every event, including:
  - Date/time of detection and reporting
  - Individuals involved
  - Actions taken during each phase
  - Lessons learned and follow-up tasks
- Store evidence securely for potential audits or legal proceedings.

10. **Post-Incident Review**

- Conduct a **post-mortem** within 1–2 weeks of incident resolution.
- Assess:
  - What happened and why
  - How effectively the response was managed
  - What can be improved (tools, training, processes)
- Update the incident response plan and related security policies accordingly.

11. **Training and Awareness**

- Conduct regular incident response training for technical and non-technical staff.
- Simulate incident response scenarios (e.g., phishing attacks, ransomware) to evaluate readiness.
- Keep the IRT's skills and tools current with evolving threats.

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

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