INFORMATION SECURITY POLICY

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

MARCH 2025

INFORMATION SECURITY POLICY

1. **Purpose**

The purpose of this Information Security Policy is to protect the confidentiality, integrity, and availability of ITEC's information assets. This policy establishes the guidelines for ensuring that information is properly managed, secured, and protected from threats that could compromise the organization's operations or reputation.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and others who access ITEC's information systems and data. This includes both physical and electronic information, as well as all IT resources such as hardware, software, networks, and cloud services.

3. **Information Classification and Handling**

a. **Classification:** All information should be classified based on sensitivity (e.g., public, internal use, confidential, and restricted).

- ✓ **Public:** Information that can be freely shared with the public without causing harm to the company.
- ✓ **Internal Use:** Information that is necessary for day-to-day operations but is not meant for public release.
- ✓ **Confidential:** Information that could harm the company or its stakeholders if disclosed.
- ✓ **Restricted:** Information that is highly sensitive and protected by law or regulation (e.g., personal customer data, financial information, intellectual property).

b. **Handling Sensitive Information:** Sensitive information must be protected at all times, both in transit (e.g., using encryption) and at rest (e.g., using password protection or encryption).
c. **Data Disposal:** Any sensitive data, whether in physical or digital format, must be securely disposed of when no longer needed (e.g., shredding paper records, wiping hard drives).

4. **Access Control**

- ✓ **User Access Management:** Access to systems and data should be granted based on the principle of least privilege, ensuring that individuals have only the access they need to perform their job duties.
- ✓ **Authentication:** Strong authentication mechanisms (e.g., multi-factor authentication) must be used for accessing sensitive systems and data.
- ✓ **Password Management:** Employees must use strong passwords (e.g., minimum 8 characters, combination of letters, numbers, and symbols) and change them regularly. Passwords should not be shared or written down.

- ✓ **Privileged Access:** Access to administrative accounts should be tightly controlled and monitored, with regular reviews of access rights.

5. **Data Protection and Privacy**

- ✓ **Personal Data Protection:** Personal data should be processed in accordance with applicable data protection laws and regulations (e.g., GDPR, CCPA). Employees must take steps to ensure that personal data is kept confidential and used only for legitimate business purposes.
- ✓ **Encryption:** Sensitive and confidential information must be encrypted when stored on devices or transmitted over the network to prevent unauthorized access.
- ✓ **Third-Party Data Sharing:** Personal or sensitive data should not be shared with third parties unless proper agreements are in place, and the third party is adequately secured.

6. **Network and System Security**

- ✓ **Firewall and Intrusion Detection:** All company networks must be protected with firewalls and intrusion detection systems to monitor and prevent unauthorized access.

- ✓ **Anti-Malware:** All devices must have up-to-date anti-virus and anti-malware software installed to prevent the introduction of malicious software into the network.
- ✓ **System Updates and Patching:** All software and systems must be regularly updated to ensure that known vulnerabilities are patched promptly.
- ✓ **Secure Remote Access:** Employees working remotely must use a secure Virtual Private Network (VPN) to access company systems.

7. **Incident Response**

- ✓ **Incident Reporting:** All employees must immediately report suspected security incidents, breaches, or vulnerabilities to the IT or security team.
- ✓ **Incident Handling:** In the event of a security incident, the company will follow a predefined incident response procedure to contain, investigate, and remediate the incident.
- ✓ **Post-Incident Review:** After an incident is resolved, a review will be conducted to determine root causes, assess the impact, and implement corrective actions to prevent recurrence.

8**. Training and Awareness**

- ✓ **Security Training:** All employees must undergo regular security training to understand their role in protecting company information and preventing security threats (e.g., phishing, social engineering).
- ✓ **Ongoing Awareness:** Employees should be regularly updated on new security threats, company security policies, and best practices for securing information.

9. **Monitoring and Auditing**

- ✓ **Continuous Monitoring:** ITEC Ltd will monitor systems, networks, and access logs for suspicious activity or security threats.
- ✓ **Audits:** Periodic security audits will be conducted to assess the effectiveness of security controls, compliance with this policy, and any potential security gaps.

10. **Compliance**

- ✓ **Regulatory Compliance:** ITEC Ltd will comply with applicable laws, regulations, and industry standards related to information security (e.g., GDPR, HIPAA, PCI DSS).
- ✓ **Internal Compliance:** Employees must adhere to this Information Security Policy and any additional policies or standards related to security.

11**. Enforcement**

- ✓ **Disciplinary Actions:** Failure to comply with this Information Security Policy may result in disciplinary actions, including but not limited to warnings, termination, and legal action if warranted.
- ✓ **Policy Violations:** Employees must immediately report any violations of this policy or any incidents that may impact the security of information.

12**. Review and Updates**

This Information Security Policy will be reviewed periodically and updated as needed to reflect changes in the company's information security needs, regulatory requirements, or emerging threats.

Acknowledgment

By accessing and using ITEC's information systems, you acknowledge that you have read, understood, and agree to comply with the terms of this Information Security Policy.

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