DATA PROTECTION POLICY

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

MARCH 2025

DATA PROTECTION POLICY

1. Purpose

The purpose of this Data Protection Policy is to ensure that ITEC Ltd complies with all applicable laws and regulations regarding the collection, use, storage, and sharing of personal and sensitive data. The policy outlines the company's approach to safeguarding data and ensuring the privacy and rights of individuals are protected.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and any other entities who process personal or sensitive data on behalf of ITEC Ltd. It covers both digital and physical data and includes all data collected in relation to employees, customers, business partners, and other individuals.

3. Data Classification

- ✓ **Personal Data:** Any information that can identify an individual, such as name, address, email, phone number, identification number, etc.
- ✓ **Sensitive Data:** Personal data that is more sensitive in nature, such as health information, financial data, racial or ethnic origin, political opinions, and biometric data.
- ✓ **Confidential Data:** Any data that is critical to the company's operations and requires protection (e.g., business contracts, financial data, intellectual property).

4. Data Collection

- ✓ **Minimization Principle:** Only data that is necessary for the purposes of the business will be collected. We will not collect excessive or irrelevant data.
- ✓ **Transparency:** Individuals will be informed about the data being collected, the purpose for which it is collected, and how it will be used. This will be communicated via clear privacy notices or agreements.
- ✓ **Consent:** Where necessary, explicit consent will be obtained from individuals before collecting their personal data, especially when processing sensitive data.

5. Data Storage and Retention

- ✓ **Secure Storage:** Personal and sensitive data must be stored in secure systems with appropriate encryption, access control, and authentication measures.

- ✓ **Data Retention:** Data will be retained only for as long as it is necessary for the business purposes for which it was collected. After the retention period, data will be securely deleted or anonymized.
- ✓ **Data Segmentation:** Sensitive data must be segregated from non-sensitive data and stored in separate systems or environments where possible.

6. **Data Access and Use**

- ✓ **Access Control:** Access to personal and sensitive data will be restricted based on the principle of least privilege, meaning that only authorized individuals will have access to data that is necessary for their role.
- ✓ **User Authentication:** Strong user authentication methods, such as multi-factor authentication, must be used to access systems containing personal data.
- ✓ **Data Use:** Personal and sensitive data should only be used for the purposes for which it was collected. Unauthorized use of data is strictly prohibited.

7. **Data Sharing and Transfers**

- ✓ **Third-Party Sharing:** Personal data may only be shared with third parties when absolutely necessary and with proper safeguards (e.g., Data Processing Agreements, Non-Disclosure Agreements).
- ✓ **International Data Transfers:** If personal data is transferred outside the country or the jurisdiction in which it was collected, such transfers will only occur when the receiving party ensures an adequate level of data protection, in compliance with applicable laws (e.g., EU-US Privacy Shield, Standard Contractual Clauses).
- ✓ **Public Disclosures:** Personal data will not be disclosed to the public or external parties unless required by law or with the individual's consent.

8. **Data Security Measures**

- ✓ **Encryption:** Personal and sensitive data must be encrypted both in transit (when being transmitted) and at rest (when stored) to prevent unauthorized access.
- ✓ **Firewalls and Security Systems:** Firewalls, intrusion detection systems, and other security mechanisms must be used to protect data from unauthorized access, data breaches, or cyber-attacks.
- ✓ **Anti-Malware and Anti-Virus Protection:** Devices and systems must be equipped with up-to-date anti-malware and anti-virus software to protect against malicious software.
- ✓ **Regular Security Audits:** Regular audits and vulnerability assessments must be conducted to ensure the effectiveness of data protection measures.

9. **Data Breach Management**

- ✓ **Incident Response:** In the event of a data breach or security incident, the company will follow an established incident response plan. Affected individuals will be notified promptly if their personal data has been compromised, in accordance with applicable regulations.
- ✓ **Breach Reporting:** All employees are required to report any data breaches or suspected security incidents immediately to the IT or security team. A breach will be investigated, and appropriate actions will be taken to mitigate the impact.
- ✓ **Regulatory Notification:** If required by law, ITEC Ltd will notify relevant authorities and regulators of any data breaches within the required timeframes (e.g., 72 hours under GDPR).

10. **Data Protection Rights**

- ✓ **Right to Access:** Individuals have the right to request access to their personal data held by ITEC Ltd and to obtain information on how it is being used.
- ✓ **Right to Rectification:** Individuals can request corrections to any inaccurate or incomplete data held about them.
- ✓ **Right to Erasure (Right to be Forgotten):** Individuals can request the deletion of their personal data, subject to legal or business requirements that necessitate retention.
- ✓ **Right to Restrict Processing:** Individuals can request the restriction of the processing of their personal data under certain circumstances.
- ✓ **Right to Data Portability:** Individuals can request to receive their personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.

11. **Employee Responsibilities**

- ✓ **Training and Awareness:** All employees must complete regular data protection training and understand their responsibilities regarding data security and privacy.
- ✓ **Compliance with Policies:** Employees must comply with this Data Protection Policy, as well as any applicable laws and regulations. Failure to comply with the policy may result in disciplinary actions.
- ✓ **Reporting Violations:** Any violations of data protection practices, including improper handling of personal data or suspected data breaches, should be immediately reported to the Data Protection Officer (DPO) or relevant authorities.

12. **Compliance with Legal Requirements**

ITEC Ltd is committed to complying with all applicable data protection and privacy laws, including but not limited to:

- The Rwanda Data Protection Regulation (RDPR)
- Other relevant data protection laws.

13. Review and Updates

This Data Protection Policy will be reviewed and updated annually or as needed to reflect changes in laws, regulations, and business operations.

Acknowledgment

By accessing and handling personal or sensitive data, employees acknowledge that they have read, understood, and agree to comply with this Data Protection Policy.

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