Information Technology Security Guideline

Our organization is committed to protecting the confidentiality, integrity, and availability of all information assets under our care. We recognize that effective information security is essential to maintaining trust, ensuring operational continuity, and meeting regulatory and stakeholder expectations.

To this end, we commit to the following principles:

- **Continuous Improvement**: We will continuously enhance our information security management systems to adapt to evolving threats, technologies, and business needs.
- **Integrity and Data Protection**: We will ensure the integrity, accuracy, and protection of organizational and customer data, applying appropriate controls to prevent unauthorized access, alteration, or destruction.
- **Threat Monitoring and Response**: We will actively monitor for information security threats and take prompt, appropriate actions to detect, mitigate, and respond to any incidents or vulnerabilities.
- **Individual Responsibility**: We will define and communicate clear roles and responsibilities for information security across all levels of the organization. All employees, contractors, and relevant stakeholders are expected to understand and fulfill their security obligations.
- **Third-Party Requirements**: We will establish and enforce information security requirements for all third parties who access, process, or store our data, including suppliers, contractors, and service providers, to ensure alignment with our security standards.

This guideline will be reviewed periodically and updated as necessary to ensure its continued relevance and effectiveness.