Information Security Policy

1. Purpose:

To strengthen information security management, ensure the confidentiality, integrity, and availability of information assets belonging to the company and its clients, and provide a secure information environment for the continuity of business operations while complying with government regulations and stakeholder requirements.

2. Scope:

The policy applies to the security management of the data center operations, business operation systems, and website maintenance to meet all security requirements and expectations.

3. Definitions:

- **Information Assets:** Include hardware, software, services, documents, and personnel essential for the company’ s operations.
- **Confidentiality:** Ensures information is accessible only to authorized users.
- **Integrity:** Ensures information and processing methods are accurate and complete.

- **Availability:** Ensures authorized users can access information and assets when needed.

4. Objectives:

- Protect business information against unauthorized access and modifications.
- Respect intellectual property and safeguard client and company data.
- Report and address all security incidents or vulnerabilities.
- Comply with legal and regulatory requirements to maintain business continuity.

5. Specific Management Measures and Preventive Actions:

- Employees must support and follow security management standards and procedures.
- Personnel, including third-party providers and visitors, must adhere to the policy.
- All parties are responsible for reporting security incidents or vulnerabilities.
- Violations will be handled based on civil, criminal, administrative responsibilities, or internal regulations.