Information Security Policy

1. Scope and Objectives: Provides principles for information security within the FocalTech to be implemented by all employees to achieve the three objectives of confidentiality, integrity, and availability.

2. Responsible Unit and Detection Procedures: The highest executive in the Information Department is responsible for identifying key risk factors annually based on internal risk assessments. These factors are regularly summarized by the Corporate Governance Committee, which, after integrating other risks, reports them to the Board of Directors based on materiality.

3. Information Security Initiatives

(1) Develop an annual information security operations plan.

(2) Execute the plan or directed projects accordingly. Conduct thorough reviews and maintain records to serve as a basis for future improvements and transfer of experience.

4. Policies and Operating Procedures

Policy Item	Description/Purpose	Operating Basis
1. Password/Passphrase Protection:	Establish password change rules within a defined system to prevent unauthorized access and protect information leakage.	Network and Electronic Media Operations Management Regulations
2. Acceptable Use:	Protect company data and files by clearly defining acceptable and unacceptable use of company information and hardware resources.	Personal Computer Software Management Regulations
3. Personal Computer Software Management:	Define email usage rules to prevent passive or active information leaks.	Network and Electronic Media Operations Management Regulations
4. Access Control:	Prevent unauthorized system access and damage. Establish controls over information access, information processing	Network and Electronic Media Operations Management Regulations

	facilities, and procedures based on information security requirements.	
5. Incident Response:	To minimize the damage caused by unexpected security incidents, establish incident response procedures and drills, and conduct regular testing.	Information System Emergency Procedures
6. Information System Emergency Procedures:	Define BYOD (Bring Your Own Device) security policies and procedures, including network usage regulations. Network and Electronic Media Operations Management Regulations	Network and Electronic Media Operations Management Regulations
7. Computer Room and Hardware Security	Specify security management related to computer room access and uninterrupted power supply.	Network and Electronic Media Operations Management Regulations

5. Information Security Awareness Promotion

(1) Management shall regularly review, formulate, approve, and publish information security policies and awareness communications.

(2) Enhance employee information security awareness through new employee training, e-learning, information security promotion, and social projects.