VI. Cybersecurity Management:

(I) Cybersecurity management framework, cybersecurity policy, specific management plans, and resources for cybersecurity management.

1. Structure of information security organization

The Computer Center is the Company's IT department. It is chaired by the chief IT officer and a number of IT professionals to plan and establish the information security policy and provide technical support for information security. It also periodically arranges awareness education for information security to reduce information security risks.

In risk management, we address risks in terms of three aspects and reduce the significance of their impact.

Item	Risk Management Plan	Risk Incident Handling	Risk Policy Improvement
Mechanism	Implementation of appropriate controls	Timely and accurate handling	Continuous risk mitigation
Specific Action	1. Antivirus and anti-hacking mechanisms 2. Breach prevention 3. Vulnerability scan, detection, and response and backup mechanisms	1. Minimization of the scope of impact and prevention of impact expansion. 2. Real-time recovery and business recovery.	1. Review based on defects 2. Proposition of improvement plans 3. Inclusion in risk management

2. Information security policy:

The following controls are implemented according to the information security policy and regulations:

(1) Account and password principles: Stringent password principles are established, periodic password change is required, and lending passwords to others is prohibited.

(2) Information hardware use: Carrying and use of non-corporate information assets and equipment are prohibited.

(3) Information software use: Employees are prohibited from installing any software not installed or unlicensed software authorized by the Computer Center.

(4) File management: The storage equipment of personal files for corporate use, physical confidential documents, and files and document information shall be properly managed, and unauthorized access shall be prevented.

(5) Mail management: Emails of unknown origins or suspicious emails shall not be open and shall be deleted immediately.

(6) Network use: No fraudulent use or diddling of the assigned IP; no unauthorized connection to the corporate network; no unauthorized erection of wireless transceiving equipment.

(7) Periodic policy announcement, case study, and awareness education of information security: Publish the related policies, case study, and awareness education of information security over the corporate network or by email to keep employees updated with and follow the information security policies.

3. Specific cybersecurity management plans and resources:

(1)Updating and improvement of IT infrastructure:

①Purchase new server hardware and software and update server and client OS to the latest version.

②Implement the vulnerability scan system to reduce information security problems from loopholes.

③Update network equipment and increase backup lines and equipment to prevent business disruption caused by the damage of single equipment or single line.

(2)Strengthening backup mechanism:

①Purchase new-model backup solutions.

②Establish new SOPs for backup, recovery, and disaster response drills.

③Build the server redundancy mechanism to reduce post-disaster downtime.

(3)Strengthening information security concept in employees:

Apart from invasion from outside, increasing information security incidents are caused by the infection of employee equipment, resulting in information security incidents of larger scale.

①Periodically announce policies, case study, and aware education of information security.

②Education and training for information security for employees to raise awareness of information security inside and outside the Company.