Cyber security management

To control or maintain important corporate operating functions, including operation and accounting, etc. functions, of the Company, the Company relies on a network system. However, the network system may be subject to network attack such that confidential information of the Company may be stolen, such as exclusive information of customers or other stakeholders, as well as personal information of employees. Malicious hackers may also try to introduce computer viruses, destructive software, or ransomware into the Company's network system, interfering with the operation of the Company in order to regain control rights of the computer system such that it may perform ransom or steal confidential information from the Company.

Countermeasures:

A. Under Administration and Management Division, the IT department periodically checks the information security of the Company, which is led by the IT department head. The IA department audits the computer cycle-information security annually and reports the audit results to the Audit Committee and Board of Directors.
B. Information Security Policy established by the Company which includes (1) Data redundancy, (2) Data storage, (3) System security, (4) level of risk, (5) authorization and (6) regulations of the system and email usage. The Company announces the policy on the intranet in order to allow all employees to access and to comply. IT department periodically evaluate the information security in compliance with the policy and report to the CEO.
C. Perform major updates of systems irregularly. In the case of major information security risks, the announcement is made, and corresponding measures are adopted. Arrange information security courses every year for training an employee to identify fishing emails. The system is protected by password, and the authentication scheme is Single sign-on which is easy to maintain and manage.
D. To strengthen network security, cope with the popularity of the Internet of Things and the information security issues associated. Reduce hazards caused by viruses, worms, and other network attacks, adopt various security preventive measures and update periodically, including the technologies of firewalls, intrusion detection systems, anti-virus software, etc., in order to respond to and reduce harm caused by various network attacks in a timely manner.
E. The information system infrastructure has been established with host machine redundancy and remote data backup mechanisms of high availability in order to ensure uninterrupted service. Perform daily data backup and store the backup at a

remote site for preservation. Enhance various simulation tests of the machine room and emergency drills in order to ensure the normal operation of information system and data security, thereby reducing system interruption risks caused by unexpected natural disasters and human errors, such that the expected system recovery target time can be satisfied. In the future, the Company will perform upgrade on selected systems for system infrastructure, expansion flexibility and disaster recovery, information security, etc. According to the risk level, design is planned and appropriate software/hardware equipment is upgraded. In addition, the storage space of remote data backup is evaluated.

F. In 2021, the IT department sent at least five newsletters or notifications to all employees, reminding employees to be alert to any abnormal letters and immediately notify IT personnel. The head of the IT department also arranges information security training courses for the IT personnel. In addition, updates and exchanges of the latest information on cyber security from related manufacturers at any time.