Information Security Risk Management Framework

Security Risk Management Team is responsible for reviewing the security policy of each subsidiary, supervising the operation of the Group's security management, and regularly reporting to the Group top management. Security Control Structure consists of subsidiary local site security and group holding security. Each site has its own local security control and group security team oversees and manages security control for the entire group. Security Risk Management covers a variety range such as in data, database, application, accessibility, security.

Information Security Policy

The main goal of the security strategy is to focus on the three aspects of security management, legal compliance and technology application, from the system to the technology, from the personnel to the organization, comprehensively improve the security protection capabilities.

In view of the current emerging trends in asset security, such as DDoS (Distributed Denial of Service) attacks, ransomware, social engineering attacks, and fake websites, we communicate with international security vendors every quarter, and regularly focus on the security issues and planning through project cooperation. In response to the plan, DDoS, and other offensive and defensive drills were carried out for different security scenarios, and the resilience of the processing personnel was strengthened, so that the blockage could be detected and completed at the first time. In addition, frequent training and classes are conducted. All users are required to participate.

In order to strengthen information security management, in addition to planning the network architecture with the most stringent requirements for security, we regularly invite external security experts for evaluation and ensure compliance with laws, such as GDPR.

Specific management plan

In order to prevent information errors from being sent to external email addresses or external connection to our network, we screen and limit traffic to domains that have potential risk. List of measurements taken but not limited to:

1. Weekly training to security administrators
2. Mobile device security control includes wipe and delete device
3. Data loss prevention endpoint - device accessibility control
4. Suspicious login and multiple devices login alerts
5. Phishing and malware protection
6. Disaster recovery

7. Regular security check up on 1) multiple devices connections, 2) devices locations, 3) 2-Step Verification

8. Password strength and length enforcement & monitoring

9. Multi-layer login verification

10. Email TLS Security Encryption

E-learning courses are available for all employees, including the general manager, to further build awareness of information security.

Conducting information security advocacy for business partners

The risk of information leakage has reached an unprecedented height. In order to respond flexibly to this, the Group has implemented Data Loss Prevention and Drive Encryption.

Responsive to cyber attacks

In order to respond flexibly to the recent security risks such as email attacks and malicious software infections, security presentations and training are conducted to all employees