Information Security Risks and Management Measures

1. Assessment and Analysis of Information Security Risk:

To respond to technological advancement and communication development and strengthen the measures taken to protect document assets of iST and its customers, iST has reviewed internal and external environmental factors.External risks are cyberattack threat and hacking while internal risks are information leak, virus, and computer room management.

2. Response Measures:

a). iST has the security control committee integrate operations of departmental security management procedures and effectively manage security incidents and prevent them from recurring, in hopes of reducing the possibility of information security risks.

b). iST has various internal management measures, such as anti-virus software, WSUS, firewall management, VLAN management, VPN management, and control mechanisms for various equipment, but iST is unable to guarantee that these measures can completely avoid all malicious attacks from third parties. However, through remote backup, computer room and network HA (High Availability) structure, and the annual disaster recovery drill, iST reviews and evaluates internal procedures to ensure appropriateness and effectiveness of system operation.

c). iST may encounter computer viruses, destructive software or denialof-access attacks, or unintentional or malicious actions of employees that may cause leak of customers’ data, or damage to customers. In light of the aforementioned circumstances, iST has introduced encryption software into its units to protect experimental conditions, results, reports and other files of customers.

d). To strengthen its information security management framework, iST obtained the ISO27001 certification in October 2020, and has used many systems, including but not limited to system vulnerability scanning and correction, social attack simulation, and log management and analysis, to ensure effectiveness of information security incident detection.

e). iST has made efforts to complete necessary facilities and established systems at all levels, but iST is unable to guarantee confidentiality, integrity and availability of information all the time in the environment filled with variable information security threats. If iST cannot solve technical problems caused by cyberattacks in real time, iST’s information system and environment may be abnormal or damaged and commitments made by iST to its customers and other stakeholders may also be compromised. Moreover, iST’ s operating results, financial conditions, prospects and reputation may also be affected adversely.