Information Security Policy

The Valuence Group (hereinafter the “Group”) recognizes that threats to information security evolve from day to day and that in an advanced society driven by information technology, protecting material information rigorously is both a social responsibility and a priority management issue that a company must address to achieve sustainable growth.

The Group hereby establishes the “Information Security Policy” to ensure the protection of its information property, and in the event that a security incident occurs to the information property, the Group will investigate the cause of the incident immediately and endeavor to minimize damage.

The Group ensures the confidentiality, completeness and availability of information security as an entire group under this Information Security Policy, as it provides its services to customers for 24 hours a day, 365 days a year. In addition, in response to changes in risk environments over recent years, the Group implements a third-party vulnerability assessment and carries out improvements and countermeasures to address risks identified in the assessment, and thereby maintains a stable supply of service.

1. Information Property

Information property means any information that the Group handles, regardless of media, in its business operations and any equipment, facility and service necessary for the Group to handle the information.

Information property specifically includes written and electronic data (including a customer’s personal information, an employee’s personnel information, a company’s financial information, contracts, various logs and records, and source code for Group companies’ internal information systems), mobile devices (including smartphones and tablet devices), and external storage media (including USB storage devices, SD cards, CDs, DVDs, and external HDDs).

2. Compliance with Laws and Regulations, Contracts, etc.

The Group complies with laws, regulations and standards relating to information property and requirements and obligations relating to information security under contracts with customers.

3. Education

The Group provides all officers and employees with education on measures to strengthen information security with reference to the information security management systems under JISQ27000. As education initiatives to raise awareness about information security, the Group implements a training program for new employees and regularly-scheduled training courses under its information security management rules, distributes learning materials on information security, and offers e-learning programs.

4. Information Security System

As part of its effort to provide safe services, the Group has in place regulations, under JISQ27000, that employees are required to observe in handling personal information and confidential information, and also implements measures to strengthen information security with reference to information security management systems. The Group has formed an information security team system that, should a security incident occur, will take actions that are commensurate with the level of the incident, analyze risks, and carry out countermeasures to address damage. In addition, after the security incident is resolved, the Group analyzes the incident again to establish a Plan-Do-Check-Act (PDCA) cycle for minimizing damage and preventing the recurrence of damage.

5. Cyber Security System

The Group has formed a security team system with Computer Security Incident Response Team (CSIRT) functions that, should a service disruption or a security incident occur, will analyze the cause of the incident, investigate the scope of impact, take actions and conduct risk analysis that are commensurate with the level of incident, and carry out countermeasures to address damage and resolve the disruption. In addition, after the disruption is resolved, the Group analyzes the incident again to establish a PDCA cycle for minimizing damage and preventing the recurrence of similar damage.

6. Security Measures in Information Systems

For each client’s device, the Valuence Group has worked to strengthen endpoint security, using Endpoint Detection and Response (EDR) and others to address unauthorized access and malware. Through these measures, the Group detects and removes unknown viruses and malware. For Internet communication, the Group has introduced a cloud proxy, and ensures security in communication, including communication with the outside of its network over the Internet in remote work etc., by implementing communication monitoring and SSL decryption. In addition, the Group has implemented DLP to detect an alert for, block, and record logs of any act by a malicious user or third party. Moreover, for personal computers and tools provided by a Group company, the Group has in place an environment in which personal information and certain websites cannot be accessed.

7. Collaboration with Outside Agencies

The Group has in place a system for collecting information security and vulnerability information from outside agencies such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and Information-technology Promotion Agency, Japan (IPA) and continuously strengthening the Group’s information security.

8. Protection of Data Privacy

The Group handles information about a customer’s address, name, occupation, age, credit card and others in its activities such as store operations and sale promotion, and records and manages personal information in books and other documents or electromagnetically.

In order to ensure compliance with the “Act on the Protection of Personal Information” and prevent the leakage of personal information, the Group has in place a system for implementing proper protection measures in handling personal information, while also working to enhance its function of personal information protection management by taking such measures as obtaining the Privacy Mark, establishing internal rules and regulations, strengthening internal management systems, providing rigorous employee education, and strengthening the security of information systems.

In addition, the Group handles personal data that is subject to the General Data Protection Regulation (GDPR) in a proper manner pursuant to the regulation.