# Information Security

## Balancing Security and Convenience

**Convenience and security often come into conflict in the development of cloud services. Yet, it is vital to maintain the best possible balance between these two elements when aiming to increase social and economic efficiency and productivity. Our corporate philosophy is to balance both security and convenience. That's why we prioritize providing secure and stable infrastructure and ensuring data privacy and information security, and consider these to be critical. We aim to minimize security risks and ensure that we can provide our services safely and securely as we pursue further growth.**

### Information Security Measures and Management System

Our services facilitate the management and use of data that includes private customer information, such as that on companies and individual users. We position the handling and protection of personal information and other vital information assets as our most critical management concern. Having formulated policies for protecting personal information and information security, we rigorously manage information assets and take every possible measure to minimize risk. In our security system, to be able to respond quickly and in all directions to privacy and security risks, executive officers themselves assume the roles of CISO[*1] and DPO.[*2] We have also set up the CSIRT,[*3] a department specializing in information security across Sansan. Since our founding in 2007, we have maintained a Personal Information Protection Management System as a measure to protect data, establishing an environment to deal with such protection within the company. We have also built a system that can continually monitor key data by fully leveraging the latest security technology.

*1 Chief Information Security Officer
*2 Data Protection Officer
*3 Computer Security Incident Response Team

### Primary Duties Related to Information Security

**CISO**

This role has responsibility and authority for the security and risk management of information systems. The person oversees information security risk measures and management methods.

**DPO**

Data Protection Officers are responsible for and authorized to operate the PMS. They are also responsible for monitoring compliance with the GDPR.

**Information System Administrator**

As the head in charge of information system management, this person executes tasks based on authorization related to organizations and divisions of duties in consultation with the CISO.

**CSIRT**

CSIRT is our group that gathers information on events that potentially threaten information security and system vulnerabilities, monitors signs of cyberattacks and other risks, and formulates response measures and procedures.

### Incident Guidelines

To prepare for incidents that may impact our services, such as disasters, accidents, unauthorized access, and vulnerability issues, we have established guidelines for each department related to incident response frameworks, chains of command and decision-making criteria, and response procedures. Specifically, we classify incidents in terms of confidentiality, integrity, and availability, set priorities for each incident we are addressing, and define staff in each department responsible for making determinations relating to incidents and incident responses.

### Education on Information Security

As part of our aim of ensuring a correct understanding of the Act on the Protection of Personal Information and safety management, all executives must acquire certification as a Protection of Individual Information Person. Salary increases are, in principle, suspended if an employee does not pass the exam after a certain period, and until they do pass. Information security and personal information protection training is provided upon hiring and then annually. These opportunities help ensure employees correctly understand the Act on the Protection of Personal Information and have systematic knowledge of safe data management. We also have strict information asset handling procedures, such as prohibiting storage of personal and confidential information on PCs. The Internal Auditing Department appoints security committee members from among employees to strengthen awareness of security through the use of a mutual security auditing system.

### Third-Party Certifications

We are committed to obtaining third-party security-related certifications and periodically renewing them. We have received various accreditations including the PrivacyMark system and international ISO/IEC standards, which strengthen our information security and give our services further credibility.

**PrivacyMark**

The PrivacyMark system is in accordance with the Japanese Industrial Standard JIS Q15001: Personal Information Protection Management System - Requirements. It certifies that entities such as businesses have established appropriate protections for personal information based on the systems guidelines for establishing and operating personal information protection management systems. Certified groups can use PrivacyMark in their business activities. We obtained certification in 2007.

**SOC 2 Type 1**

SOC 2 reports are performed following Trust Services Criteria established by the American Institute of Certified Public Accountants. In these reports, which are not limited to financial matters, auditors express their opinions on internal controls. Areas examined include either security, availability, processing integrity, confidentiality, or privacy. Deloitte Touche Tohmatsu LLC has issued a report on internal controls for Type 1 security at Sansan.

**Legal Requirements for Electronic Transaction Software Certification**

The Japan Image and Information Management Association's Legal Requirements for Electronic Transaction Software Certification System checks whether software and software services that create and electronically exchange national tax-related documents comply with the Electronic Book Storage Act. Bill One and Contract One were certified in April 2022.

**ISO/IEC 27001 and ISO/IEC 27017**

In May 2022, Sansan and Bill One acquired ISO/IEC 27001 certification, an international standard for information security management systems. At the same time, Sansan also acquired ISO/IEC 27017 certification, an international standard for cloud security applicable to cloud service provision and use.

### Technical Security Initiatives

We implement a variety of security measures including vulnerability assessments and penetration testing, which third-party organizations and specialized in-house departments perform.

**Encryption of All Data Center Transmissions**

Alongside establishing firewalls, all external transmissions to our data center are highly encrypted using user-authenticated HTTPS.

**Images Are Deleted After Business Cards Are Scanned**

Sansan scanners are installed with software that prevents unauthorized external access. After business cards are scanned, the image data is deleted from the scanners.

**Vulnerability Assessments and Penetration Testing by Security Specialists**

We appoint external organizations to test our security through penetration testing based on the identification of system vulnerabilities and cyber-attacks, and to correct problems and otherwise strengthen our services.

**High Service Availability**

All our servers are load-balanced. Services can be promptly restored in the event of a failure. Additionally, our data centers are redundantly configured to minimize the risk of functional and service outages in the event of a disaster.