Information Security

Basic Approach

Approach Policy

We control information security and cyber security across the Group in the recognition that the appropriate and safe management of information and systems necessary for our business is a significant managerial challenge for TOPPAN as we grow as a leader in providing solutions to global social issues.

The threat of cyber-attacks has been mounting with the advancement of the IoT and rapid digital transformation. These attacks can result in the leakage of information assets, including personal information or confidential information, and endanger business continuity per se.

In keeping with the TOPPAN Group Basic Policy on Information Security and the Personal Information Protection Policy, we apply secure technologies and rigorous control in operations throughout the Group to reciprocate the trust of customers and society and drive a digital transformation that enhances our corporate value. We have been introducing various systems and tools to counter cyber-attacks and reinforcing safeguards across the tightly secured areas designated for the handling of personal information throughout Japan.

More details on the TOPPAN Group Basic Policy on Information Security ›

https://www.holdings.toppan.com/en/about-us/our-corporate-approach/security-information.html

More details on the Personal Information Protection Policy ›

https://www.holdings.toppan.com/en/privacy.html

TOPPAN Group Basic Policy on Information Security

As a group of companies operating in the information communication industry, each of us at the TOPPAN Group carries out Groupwide information security management in the recognition that the management of information necessary for business is a significant managerial challenge for us as a means to reciprocate our customers' trust and promote the ongoing growth of the TOPPAN Group.

1. We manage information necessary for our business appropriately in observance of our in-house rules, the law, and the principles of social order.
2. We collect information for appropriate purposes using appropriate methods.
3. We safely manage the information entrusted to us by customers in order to reciprocate our customers' trust.
4. We are deeply aware of the risks to the information assets we handle, such as illegal access, loss, damage, falsification/manipulation, and leakage of information, and take necessary and reasonable safety measures against these risks. We deal with and rectify any problems that occur promptly and in an appropriate manner.
5. We establish, operate, maintain, and continuously improve information security management systems.

Established on April 1, 2001
Revised on June 27, 2019

Hideharu Maro
President & Representative Director
Toppan Inc.

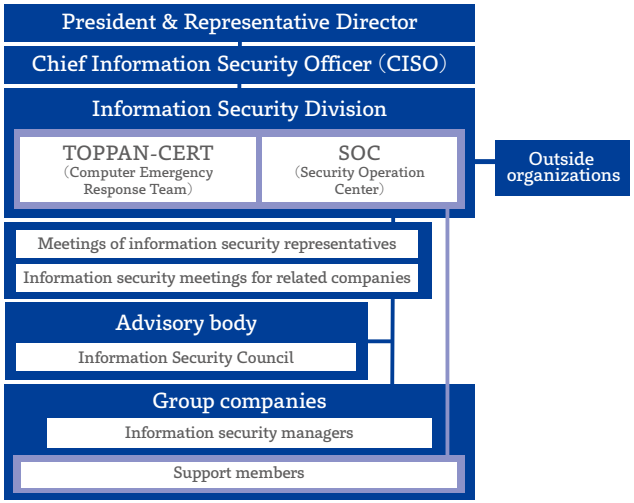
Promotion Framework

Promotion framework

The Director in charge of the Information Security Division has been appointed as the Chief Information Security Officer (CISO) of the Group. The Information Security Division practices information security governance on the technical front, while cross-functional specialist teams control cyber security by overseeing Group companies in cooperation with outside expert organizations.

In parallel, information security managers in Group companies work to manage the safety of their organizations according to the instructions issued by the Information Security Division.

Organizational Structure for Information Security Management



Information Security Management Structure

Promotion framework

Information Security Management

Under the Chief Information Security Officer (CISO), the Information Security Division formulates a Groupwide information security plan, sets up rules and regulations, and disseminates and reviews them. The division convenes regular meetings with members from Group companies to share the details of our information security policies and measures underway.

The Information Security Division also carries out regular audits of Group companies to check the quality of their security control and recommend corrective measures as necessary.

The results of these activities are regularly reported to the CISO. When a security incident arises, the division promptly initiates a response to the incident and reports the present status to the CISO, as required.

Arranging Remote Working Environments

We have reviewed our information security rules for remote working and formulated standards for the use of communication tools to ensure safe working environments outside of the office. A system has been introduced to enable employees to promptly report suspicious incoming emails and virus-infection incidents while working from remote locations.

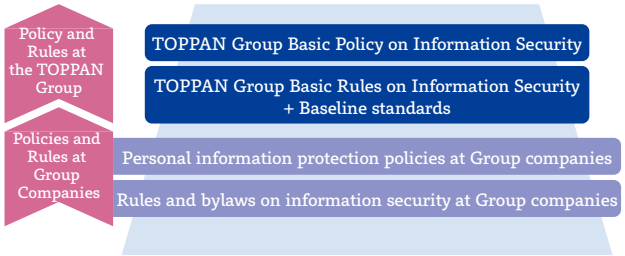
Remote approaches have also been adopted for internal audits and audits of various other types to confirm information security management throughout the Group.

Enhancing Security Governance

Our rules on information security governance have been established based on the ISO/IEC 27000 standard for information security management systems (ISMS) and comply with the JIS Q 15000 standard for personal information protection management systems (PMS).

We strive to enhance security governance throughout the global Group by better responding to emerging requirements in areas such as cyber security, the use of data, the IoT, and globalization. We are upgrading the quality of security control at Group companies by assessing the levels of control once a year with a set of baseline standards for evaluating conformance with the TOPPAN Group Basic Rules on Information Security. Improvement plans in place at Group companies, as well as their implementation, are duly monitored.

Information Security Policies and Rules



Complying with Laws and Regulations

Activity results, performance data

We comply with laws and regulations related to privacy, confidentiality, and the protection of personal information not only in Japan, but in all of the countries where Group companies operate.

Japan's Amended Act on Personal Information Protection

Our rules on information security management related to the handling of personal information have been revised to ensure compliance with the amended Act on the Protection of Personal Information enforced in Japan in April 2022. We have also set up procedures for handling personal information and anonymously processed information, notifying individuals when their information is provided to third parties outside of Japan, and submitting incident reports whenever necessary. The procedures are closely modeled after the guidelines announced by the Personal Information Protection Commission of Japan.

Overseas Legislation on Privacy and Personal Information

With the growing awareness of the importance of privacy and personal information, laws and regulations to protect them have been introduced around the world. We are taking appropriate measures to comply with these laws and regulations by collecting information and conducting surveys on the relevant legislation in the countries and regions where Group companies do business.

PrivacyMark Accreditation and ISMS Certification in Japan

Information security systems within domestic Group companies have received PrivacyMark accreditation and information security management system (ISMS) certification.

We are formulating in-house rules, building environments, and training personnel in charge of information security to secure the handling of important information received from customers, personal or otherwise.

Japan's Individual Identification Number System

New requirements for security control measures have been added to our in-house standards for tightly secured areas in accordance with the guidelines for the proper handling of specific personal information issued by the Japanese government's Personal Information Protection Commission. These security measures cover operations involving specific personal information, such as the handling of individual identification numbers under Japan's Social Security and Tax Number System and the collection of those numbers on behalf of our client companies.

Rooms dedicated to the handling of these personal identification numbers have been set up, and a special team carries out accreditation audits on operations performed therein.

Protecting Personal Information and Confidential Information

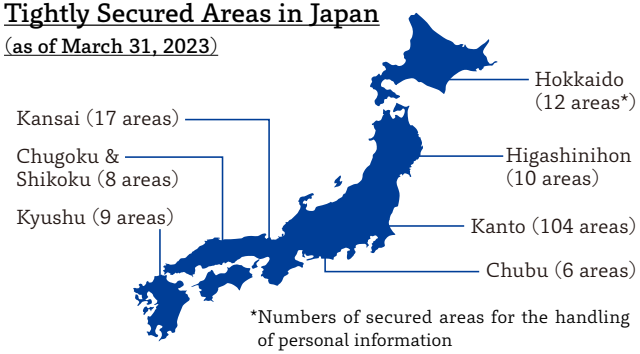
Activity results, performance data

Setting up Tightly Secured Areas

Our operations involving the use of confidential materials are conducted exclusively within workplaces that are tightly secured by access controls and other security measures in a closed network environment, in order to minimize the risk of fraudulent acts and other forms of misconduct inside of the Group and the risk of unauthorized access from outside of the Group. Strictly controlled operations include the handling of personal information (e.g., individual identification numbers under Japan's Social Security and Tax Number System) and the production and handling of security printing products with monetary value.

We found no instances of unauthorized information removal or other personal information-related incidents in fiscal 2022. Strict efforts to maintain our record of zero-incidents across the Group will continue.

Tightly Secured Areas in Japan
(as of March 31, 2023)



Controlling the Tightly Secured Areas

We constantly upgrade security levels for the handling of personal information and confidential information through regular internal audits and day-to-day operational checks based on the rules for managing the tightly secured areas within the Group. The key security management measures are described below.

Operational management inspection through internal audits: Dedicated auditors regularly inspect the installation, management, and operation of tightly secured areas. The findings of inspections are assessed and accredited to maintain and further enhance operational management levels across the Group.

Access control: Each tightly secured area is protected by technical safeguards to prevent unauthorized persons from entering. The safeguards consist mainly of personal authentication measures and controls to inhibit the entry of two or more persons at the same time.

Lockers and secure storage compartments for personal belongings are provided outside of the areas, as persons entering are not allowed to bring in cameras, cell phones, smartphones, or other devices that record or communicate images, videos, audio, or any other form of data.

Area control: Surveillance cameras eliminate blind spots in the tightly secured areas and monitor any unauthorized removal or transport of data.

Device control: As a basic rule, we prohibit employees from connecting any external storage media to devices used within the tightly secured areas. We also deploy a two-factor authentication login system requiring the submission of an ID, a password, and one or more additional factors for entry into a secured area.

Our monitoring center operates a log management system to carry out operational log analysis. Whenever a potentially fraudulent log is detected in the stored data, the center immediately notifies the relevant management personnel for verification.


Surveillance camera


Access control

Controlling Security across the Supply Chain

Some of our operations that involve the handling of personal information and confidential information are entrusted to Group and partner companies. We also rely on the cloud services of external companies in the execution of some of our business operations.

We mitigate supply chain risks by checking the safety of cloud services and deploying a system to certify business partners who take appropriate security measures. The control levels required of business partners to satisfy the security standards under our certification system depend on the types of information and operations entrusted to them.

Managing Information Assets in Internal Operations

Information assets handled in internal operations are classified by confidentiality. Our rules governing storage, removal, disclosure, etc. ensure the safe handling of information assets in line with their classifications.

Countering Cyber-attacks

Activity results, performance data

Cyber-attacks pose especially significant security risks to the Group. We have been implementing various measures to mitigate them.

Protecting PCs and Servers with the EDR Application

In fiscal 2019 we began installing Endpoint Detection and Response (EDR), an application that detects suspicious software behaviors in PCs and servers. The EDR application is now installed in PCs used for administrative work, terminals used onsite in production settings, and on the Apple computers and network servers running across the Group. The combined use of the application with data such as network logs further solidifies our information security system to ensure prompt detection and defensive action against sophisticated malware whenever a threat emerges.

Using a CASB Service to Mitigate Cloud-usage Risks

The growing usage of cloud services is driving up the amount of important information handled by cloud-based applications. Since fiscal 2020 we have been using a Cloud Access Security Broker (CASB) service that visualizes and controls computer usage in cloud environments. CASB enhances the safety of cloud-service usage by identifying risks associated with individual cloud services and detecting and restricting cloud usage subject to unduly high risk.

Implementing Threat Intelligence and OSINT Activities

We continue to implement threat intelligence, third-party evaluations, and Open Source Intelligence (OSINT) activities to uncover signs of cyber-attacks against the Group and detect vulnerabilities visible to outside parties early on. We strive to mitigate cyber-attack risks by addressing weaknesses detected within the Group before attacks can occur.

We are enhancing cyber security throughout the supply chain. Business partners entrusted with operations involving the handling of personal and confidential information have been subject to our vulnerability-detection measures since fiscal 2022.

Upgrading Website Vulnerability Assessments

Weaknesses in our web applications have been assessed to counter cyber-attacks targeting website vulnerabilities. An automatic vulnerability detection system is now installed to periodically check the network and address vulnerabilities that become apparent from day to day. This monitoring system works synergistically with various external vulnerability-detection services to further solidify our web-based services and reinforce our ability to provide clients with more tightly secured services.

In fiscal 2022 we began organizing vulnerability training sessions for employees not only in the development departments, but also the sales and sales-promotion departments, to ensure website security from the planning and design stages.

Formulating Guidelines to Address Cyber Emergencies

Cyber threats have been escalating across borders. Their unprecedented malice and technical cunning can result in instant and severe damage in all directions. In many instances, the conventional methods used against cyber-attacks are useless.

We have formulated a set of guidelines that summarize our basic approach, preparations, and action flows to address serious information security incidents caused by cyber-attacks and other destructive acts. We are constantly strengthening our responsiveness to cyber emergencies on the assumption that unforeseen incidents can always happen.

Countering Email Attacks

Cyber-threats continue to grow with the return of the malicious botnet Emotet and the rising frequency of fraudulent emails and business email compromise (BEC) crimes, where a cyber-criminal sends an email that appears to come from a familiar business acquaintance with the intent of stealing money or specific information. In fiscal 2022 we added another tool to combat these threats by introducing an advanced service that screens incoming emails with help from AI analysis and machine learning algorithms. This service blocks a high percentage of targeted email attempts to steal money, exploit information, or compromise networks in other ways. We will continue shoring up our systems to resist email attacks throughout the Group by providing this screening service to more of our Group companies from fiscal 2023 onward.

Enhancing the Capabilities of TOPPAN-CERT

TOPPAN-CERT is a specialized cyber response team made up of specialists from across the Group. In December 2022 the team participated in a series of collaborative cross-sector drills organized by the Nippon CSIRT Association (NCA) and the National center of Incident readiness and Strategy for Cybersecurity (NISC). CERT members took the lead in responding to simulated cyber-attacks targeting the TOPPAN Group. Response procedures during the drills were reviewed to pinpoint weaknesses in our counter capabilities and clarify the improvements that can best enhance the handling of a cyber-attack.

Sharing Information on Cyber Security Preparedness

We hold quarterly cyber-security information-sharing sessions for personnel involved in information security management to heighten the understanding of cyber security preparedness within and outside of the Group.

Acquiring Third-party Certification

Activity results, performance data

Toppan Inc. and Group companies have acquired ISO/IEC 27001 certification for information security management systems (ISMS), PrivacyMark accreditations under Japanese Industrial Standards (JIS) Q 15001:2017 for personal information protection management systems (PMS), and other third-party certifications, as shown in the following tables (as of June 30, 2023).

ISMS Certification (ISO/IEC 27001) for Information Security Management Systems

Information & Communication Division (Toppan Inc.); Business Platform Department (Digital Innovation Division, Toppan Inc.); Technical Department (Integration Business Center, DX Design Division, Toppan Inc.); Toppan Communication Products Co., Ltd.; Toppan Graphic Communications Co., Ltd.; TGS Inc.; TB Next Communications Co., Ltd.	IC06J0151
TOPPAN Group Kansai Business Center (TOPPAN Edge Inc.)	JQA-IM0137
Toppan Infomedia Co., Ltd.	JUSE-IR-404
Asaka Plant and Shiga Plant (Toppan Inc.); Semiconductor photomask operations (Asaka Plant and Shiga Plant, Toppan Electronics Products Co., Ltd.); Design, development, commissioned manufacture, and management of products related to semiconductors (Toppan Technical Design Center Co., Ltd.)	IS 530416
ONE COMPATH Co., Ltd.	IS 533218
Kyushu, Chugoku & Shikoku Team and ISMS Promotion Committee (Information Security Management, Nishinihon Division, Toppan Inc.)	I308
Kansai Production Department (Toppan Graphic Communications Co., Ltd.)	IC13J0361
Higashinihon Division (Toppan Inc.)	IS 606897
Takino Plant (Toppan Communication Products Co., Ltd.); Takino Information & Communication Production Engineering Team (Kansai Technology, Kansai Subdivision, Toppan Inc.)	IC14J0376
Secure BPO Team (Chubu Division, Toppan Inc.); Chubu Production Department (Toppan Graphic Communications Co., Ltd.); Nagoya Plant (Toppan Communication Products Co., Ltd.)	IC17J0444
One undisclosed entity	

ISMS Certification (ISO/IEC 27017) for Cloud Security Management

Team 3 (Development Department I, ICT Development Center, DX Design Division, Toppan Inc.)	SC22J0025

PrivacyMark Accreditations (JIS Q 15001:2017)

Toppan Inc.	10190891
Toppan Communication Products Co., Ltd.	24000216
Toppan Graphic Communications Co., Ltd.	10190298
Toppan Editorial Communications Co., Ltd.	24000308
Toppan Logistics Co., Ltd.	10450006
Toppan Travel Service Corp.	10450093
TOPPAN Edge Inc.	10190934
Toppan Forms Central Products Co., Ltd.	24000366
Toppan Forms Tokai Co., Ltd.	24000204
Toppan Forms Kansai Co., Ltd.	24000101
Toppan Forms Nishinihon Co., Ltd.	18860028
TOPPAN Edge IT Solutions Inc.	10820089
TOPPAN Edge Services Inc.	10450002
Toppan Forms (Hokkaido) Co., Ltd.	10190307
TOSCO Corp.	11820447
J-SCube Inc.	10860018
Tosho Printing Co., Ltd.	24000032
Tokyo Shoseki Co., Ltd.	10190966
Livretech Co., Ltd.	10190035
Tokyo Logistics Co., Ltd.	10860071
EduFront Learning Research Co., Ltd.	10861827
Froebel-Kan Co., Ltd.	24000369
BookLive Co., Ltd.	28000007
T.M.G. Challenged Plus Toppan Co., Ltd.	24000419
ONE COMPATH Co., Ltd.	24000445
Toppan Cosmo, Inc.	24000449
UNIWORX Co., Ltd.	21004696
Kirihara Shoten K.K.	24000459
TB Next Communications Co., Ltd.	24000464

Information Security Training

Training, education

Our extensive training and self-assessment initiatives are grounded in the belief that solidified human assets reinforce our information security management structure.

Training Employees throughout the Group

Annual training is organized to improve the security capabilities of all Group employees. In fiscal 2022 we established a program entitled, “Surfing on the changing currents: Groupwide counter-attack on information security threats in cyber and physical worlds.” The training covers comprehensive topics, from cyber-attack preparedness and daily security practices to business-division-specific risks and compliance with Japan’s amended Act on the Protection of Personal Information.

Organizing Security Training for Plant Engineers

We launched a program called the “technical-guard training school” in fiscal 2021. This program aims to achieve manufacturing DX with solidly secured production sites. Trainees learn the requirements of the safeguards deployed to protect manufacturing equipment during the processes from installation planning to disposal. Twenty employees completed the program in fiscal 2022.

Alerting Senior Management to Cyber Emergencies

Our senior management takes part in drills twice a year to rehearse the actions to take in the event of a severe cyber-attack. The drills are designed to better equip them with the leadership skills essential to control cyber emergencies.

After each drill we evaluate the results and identify challenges for senior managers in order to fortify their control capabilities during cyber emergencies.

Implementing Groupwide Self-assessment

We are asking all Group employees to check their daily security practices. Our Groupwide self-assessment initiative aims to heighten awareness on information security management by encouraging employees to reflect on their own behaviors. Self-assessment results are delivered to each department to enable the department managers to initiate improvement measures at their workplaces.

Several questions were added to the fiscal 2022 questionnaire to remind employees accustomed to remote working of the appropriate procedures for the handling of media and documents that contain confidential information. The questions are continuously updated to reinforce individual security readiness in the latest working environments.

Developing a Security Training Platform

TOPPAN Security Awareness Training (TSAT) has been formulated as a security-training platform since fiscal 2022. TSAT allows employees to repeat the steps of drill, evaluation, and training. Human asset solidification through this efficient platform reinforces cyber-attack resistance throughout the Group.

Holding Drills to Address Virus-infected Emails

We hold suspicious email reporting drills twice a year. To prepare for the drills, users of Group email addresses (about 25,000 persons in total) are requested to add a shortcut link or icon that can be quickly clicked on their standing screens to report suspicious messages they have received or already opened. In fiscal 2022 overseas subsidiary employees were asked to participate in the drills in parallel with employees from domestic subsidiaries and affiliated companies, expanding the coverage to about 50,000 persons in total.

The training was demanding. Our cyber security team sent out a fraudulent email to employees without pre-warning. Some employees clicked a URL link to a fraudulent website, failing to recognize it was fake.

Providing DOJO Training for Cyber Security Specialists

We have founded Armoris Co., Ltd., a company specialized in providing client companies and public-sector entities with programs to nurture cyber security specialists, as well as services geared to improving the security levels of their organizations. Armoris operates a series of practical personnel-training programs, including DOJO, DOJO Lite, DOJO Shot, and DOJO CORE.

The training programs at the DOJO are tailored to individual skills through methods suited to long-term, continual practices. DOJO Lite and DOJO Shot, meanwhile, arrange case examples and case studies examining the latest cyber security themes. DOJO CORE provides practical simulation drills on responding to actual incidents. Armoris strives to enhance the security capabilities of individuals and organizations throughout Japan, including the TOPPAN Group, through the DOJO programs.

Overview of Armoris’s DOJO service (in Japanese)