Information Security

Basic Approach

Approach | Policy

Toppan has reinforced safeguards to prevent leaks and outflows of personal information in diverse operations throughout the Group by restricting the handling of personal information to tightly secured areas that satisfy rigorous criteria for qualification audits. The Group has also worked for thorough security control in operation design and quality assurance for products with safe, secure systems and processes designed to manage personal information.

Toppan has declared that "each of us at the Toppan Group carries out Groupwide information security management" in its basic policy on information security. Under the basic policy, Toppan has continuously upgraded the Group's systemized rules formulated based on ISO/IEC 27001 (a stringent, globally recognized standard on information security management) in compliance with Japanese Industrial Standards (JIS) Q 15001 (a standard for accrediting PrivacyMark Systems for personal information protection management).

Toppan Group Basic Policy on Information Security
https://www.toppan.com/en/about-us/our-corporate-approach/security-information.html

Personal Information Protection Policy
https://www.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.

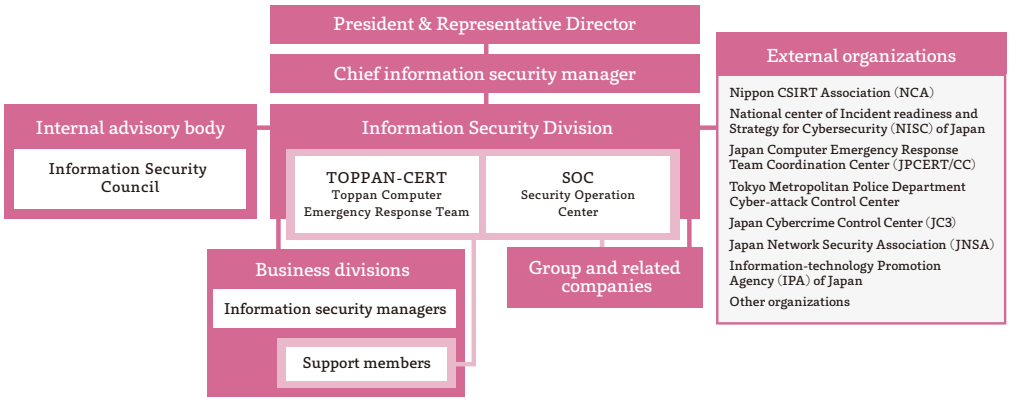
Promotion Framework

Promotion framework

Companies today face wide-ranging information security risks, from careless mistakes and fraudulent acts committed in-house to cyber-attacks and hidden threats in new business fields.

The head office and every business division at Toppan work to strengthen cooperation with relevant departments throughout the Group. Toppan seeks to secure the Group's information security governance structure through cooperation that goes beyond existing organizational boundaries.

Organizational Structure for Information Security Management



Information Security Management Structure

Promotion framework

Employing an Information Security Management Structure

Under the chief information security manager, the head office 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 the Toppan business divisions, Group companies, and related companies to share the details of information security polices and measures underway.

The Information Security Division also carries out regular audits of business divisions, Group companies, and related companies to check the quality of their information security management and recommend corrective measures to enhance their performance, as necessary.

The results of these activities are regularly reported to the chief information security manager. When a security incident arises, the division initiates the Group's response and reports the present status to the security manager as required.

Preventing the Spread of COVID-19

Toppan has reviewed the Group's information security rules for remote working and formulated standards for the use of communication tools in an effort to ensure a safe working environment without in-person interactions.

For regular training on information security management, the Group has shifted from in-person lectures to e-learning-based programs. Remote approaches were also adopted for internal audits and audits of various other types.

Reviewing In-house Rules to Improve Groupwide Information Management Systems

The Toppan Group's rules and regulations on information security management have been established based on the ISO/IEC 27001 standard for information security management systems (ISMS) and comply with the JIS Q 15000 standard for personal information protection management systems (PMS). To sustain its ISMS and PMS, Toppan needs to ensure robust governance on information security management throughout the entire Group, including overseas sites, and to respond to emerging requirements in areas such as cyber security, the use of data, the IoT, and globalization.

Common information security management rules were formulated in fiscal 2020, with plans for Groupwide application in fiscal 2021.

Complying with Laws, Regulations, Standards, and their Amendments

The Toppan Group complies with the amended Act on the Protection of Personal Information of Japan, the revised Japanese Industrial Standards (JIS) standard for accrediting PrivacyMark systems, the recently enforced EU General Data Protection Regulation, and other information-protection legislation around the world.

Complying with the Amended Personal Information Protection Law in Japan

The Toppan Group formulates rules to ensure compliance with the amended Japanese Act on the Protection of Personal Information, a law promulgated in June 2020. When the amended act comes into force, the Group will 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 to be established will be closely based on the guidelines to be announced by the Personal Information Protection Commission of Japan by April 2022.

Complying with the Revised JIS Q 15001:2017

In 2017 the Japanese Standards Association (JSA) revised JIS Q 15001:2017, a standard for accrediting a business operator or other entity with an appropriate system for the protection of personal information.

The Toppan Group has joined an inter-business project to compile a handbook on the revised standard in order to spread the relevant information throughout the printing industry in Japan. Toppan also provides Group companies with guidance on the formulation of a personal information protection system that meets the requirements for PrivacyMark accreditation under the revised standard.

Complying with International Legislation on Personal Information Protection

To address globalized business operations, Toppan specifies the Group's global standards on personal information management in accordance with the core principles of the General Data Protection Regulation (GDPR) issued by the EU. Toppan seeks to handle personal information in conformance with the applicable legislation of every relevant country.

Complying with PCI DSS for Credit Card Information Management

The Toppan Group follows the principle of "not storing cardholder data" for credit card issuance operations. In addition to the Payment Card Industry Card Production (PCI CP) standard applied to the production of credit cards, the Group works to comply with the Payment Card Industry Data Security Standard (PCI DSS) applied to the data centers that store and manage card data.

Protecting Personal Information

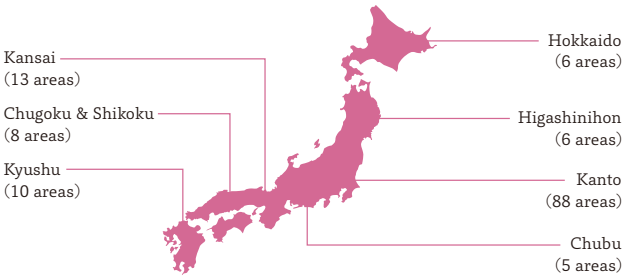
Activity results, performance data

Setting up Secured Areas for the Handling of Personal Information

Operations involving the use of confidential materials in the Toppan Group are conducted exclusively within a closed network environment and in tightly secured workplaces where the comings and goings of employees through entrances and exits are monitored 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.

Toppan found no instances of unauthorized information removal or other personal information-related incidents in fiscal 2020. The Group will continue its efforts to maintain a record of zero-incidents.

Tightly Secured Areas Where Personal Information Is Handled (as of March 31, 2021)



Controlling Secured Areas for the Handling of Personal Information

The Toppan Group seeks to ensure and upgrade security levels in the handling of personal information through regular internal audits and day-to-day operational checks based on operational rules prescribed for the tightly secured areas within the Group.

Two key components of Toppan's security management regime are internal audits to inspect operational management and monitoring to detect fraudulent operations.

Operational management inspection through internal audits:
Dedicated auditors regularly inspect the installation, management, and operation of tightly secured areas designated for the handling of personal information. Managers assess and accredit inspection results to maintain and further enhance operational management levels across the Toppan Group.

Detection of fraudulent operations:
As a basic rule, Toppan prohibits Group employees from connecting any external memory media to the PCs used within the tightly secured areas. The Group's monitoring center carries out operational log analysis using log management systems. Whenever a potentially fraudulent log is detected, the center immediately notifies the relevant management personnel for verification.

Security Measures


Surveillance camera


Access control

Countering Cyber-attacks

Activity results, performance data

Cyber-attacks pose especially significant security risks to Toppan. The Group has been implementing various measures to mitigate them.

Installing an EDR Application on PCs across the Group

In 2019 Toppan began installing Endpoint Detection and Response (EDR), an application that detects suspicious behaviors in PCs. The application is now installed in all PCs used for administrative work across the Group. The next step will be to install the EDR application on terminals used onsite in production settings, as well as on Apple computers and network servers. Toppan will continue to strengthen the Group's system for detecting and responding to sophisticated malware.

Adopting 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. The Toppan Group has adopted a Cloud Access Security Broker (CASB) service that visualizes and controls computer usage in cloud environments. Toppan is using the CASB service to enhance the safety of cloud-service usage by identifying risks associated with individual cloud services and detecting uses of the cloud that are subject to unduly high risk.

Instituting Threat Intelligence and OSINT Activities

The Toppan Group has implemented threat intelligence to uncover signs of cyber-attacks early on. The Group has also begun Open Source INTellignce (OSINT) activities to detect vulnerabilities visible to outside parties and implement preemptive security measures before an attack occurs. Toppan will continue using the OSINT techniques to reinforce cyber security across the Group.

Upgrading Website Vulnerability Assessments

Toppan has been internally assessing weaknesses in the Group's web applications to counter cyber-attacks targeting website vulnerabilities. The Group has also developed an in-house network diagnosis (platform diagnosis) system to detect vulnerabilities with operating systems and other software. With this system, Toppan is now capable of internally assessing server vulnerabilities at every level to promise customers more tightly secured services.

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.

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 Forms Co., Ltd.	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 Forms Operation Co., Ltd.	10820089
Toppan Forms Logistics and Services Co., Ltd.	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

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 Forms Co., Ltd.)	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	

Information Security Training

Training, education

Intensifying Training and Self-assessment

Toppan organized regular training on information security in fiscal 2020. The training theme for the year was “Ensuring security for customers, creating value for society.” Participants learned about evolving information security risks in and around the Group by reviewing materials from the latest *Information Security Management Guidebook* in training sessions on recent security incidents reported in society at large.

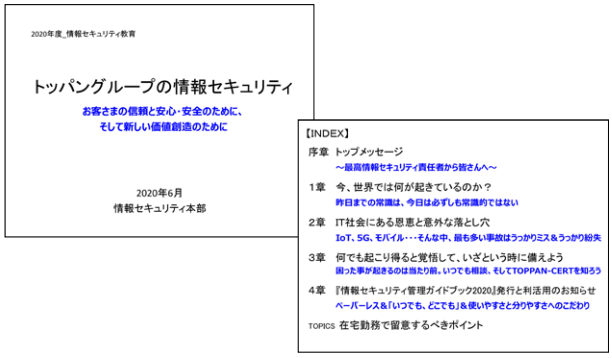
Attuned to working styles diversified under the COVID-19 restrictions, many of the group sessions were shifted from face-to-face settings to e-learning-based programs, especially for users of Toppan email addresses.

For employees engaged in production, Toppan arranged e-learning courses focused on specific risks on manufacturing premises.

The Group also held division-specific training, along with training sessions for persons handling individual identification numbers under Japan’s Social Security and Tax Number System.

In parallel with training, Toppan works on a self-assessment initiative to ensure information security across the Group. This initiative aims to enhance individual awareness of everyday behaviors by visualizing the actual state of security management to a level of detail not discernible by internal audits. Reviewing self-assessment reports sent in from different departments, the Group offers managerial staff suggestions for improvement and encourages them to take necessary actions at their workplaces.

A checklist of items to confirm risks involved in working from home was added to the Groupwide self-assessment in fiscal 2020.



Content used for a regular training course in fiscal 2020 (in Japanese)

Self-assessment report on information security in fiscal 2020 (in Japanese)

Fostering Cyber Security Specialists with Ongoing Armoris DOJO Training

In September 2019, the Toppan Group 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.”

Training programs at the DOJO are tailored to individual skills in an environment 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)

Sharing Information on Cyber Security Preparedness

Toppan continued to hold quarterly cyber-security information-sharing sessions for Group personnel involved in information security management in fiscal 2020. Toppan aims to heighten the understanding of cyber security preparedness within and outside of the Group.

Staying on Alert for Cyber Incidents

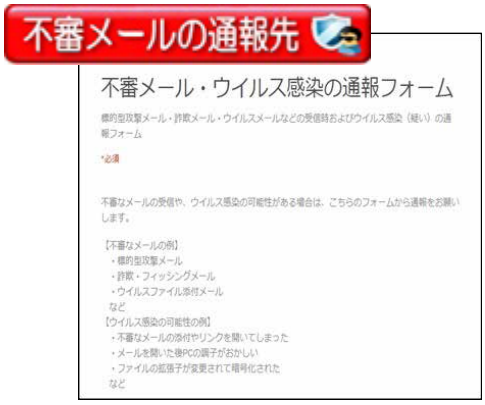
Training, education

Upgrading Suspicious Email Reporting Drills

Toppan conducted a series of suspicious email reporting drills in July 2020. To prepare for the drills, the Group requested all users of Toppan email addresses (about 21,000 users in total) to add a shortcut link or icon that could be quickly clicked on their standing screens to report suspicious emails. The drills were expanded to include about 33,000 persons at Group subsidiaries and affiliated companies in the course of the year.

Toppan held reporting drills of two different levels of difficulty in January 2021. Participants were divided into those who clicked on a link in a suspicious email sent out in the July 2020 drill, and those who did not. The training was pitched at different levels for the two groups.

Thanks to these efforts, Toppan ensured that the number of leakage incidents caused by cyber-attacks was zero in fiscal 2020, setting a benchmark to meet going forward.



Screenshot of the suspicious-email report form on the Group's internal portal site (in Japanese)

Alerting Senior Management on Cyber Emergencies

Toppan Inc. conducts annual drills for senior management to rehearse the actions to take in the event of a cyber-attack. To fortify their safeguards, the drills better equip senior managers with leadership skills to control cyber emergencies. The drills also aim to identify any challenges they may face in their efforts to shore up the Group's risk management capabilities.

Cyber security drill for senior management

Preparing for the Tokyo 2020 Games

As large-scale, international sporting events, the Olympic and Paralympic Games are easy targets for organized criminals.

Toppan Inc., a Tokyo 2020 Official Partner, gathered relevant information and took part in cross-sector, anti-cyber-attack drills organized by the Nippon CSIRT Association and the National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan.