Information Security

Basic Approach

Approach Policy

We control information and cyber security across the Group to ensure the appropriate and safe management of business information and systems as we develop into a leading provider of solutions for global social issues.

The threat of cyber-attacks has been mounting with the rapid advancement of IoT and digital transformation. Attacks can result in the leakage of personal or confidential information assets and endanger business continuity. 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 introduce systems and tools to counter cyber-attacks and reinforce safeguards in the secured areas designated for the handling of personal information throughout Japan.

More details on the TOPPAN Group's 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 October 1, 2023

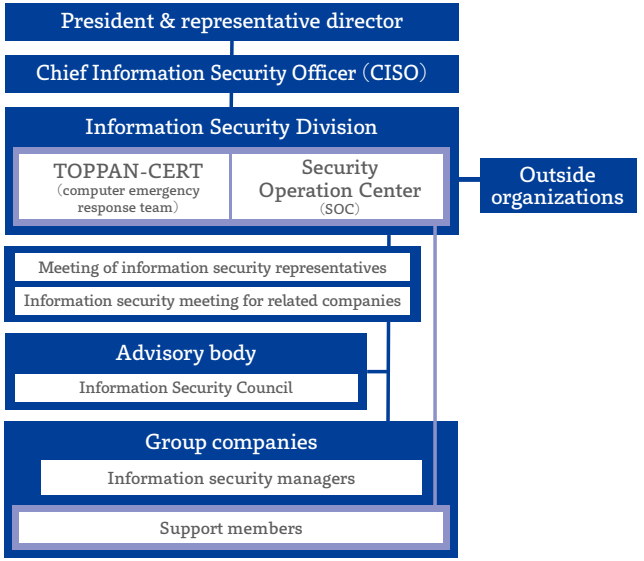
Hideharu Maro
Representative Director, President & CEO
TOPPAN Holdings Inc.

Promotion Framework

Framework

The officer in charge of the Information Security Division serves as the Chief Information Security Officer (CISO) of the Group. The Information Security Division implements information security governance and technical measures. Cross-functional specialist teams control cyber security by overseeing Group companies jointly with outside organizations. Information security managers at Group companies manage the safety of their organizations according to the instructions of the Information Security Division. The meeting of information security representatives and the information security meeting of related companies are held twice annually. The CISO and information security managers from organizations across the Group gather at these meetings to share and check the plans and results of security measures formulated based on the Group's information security strategy. Information security personnel from the main operating companies also convene an Information Security Council every month to issue advisories and share information on security measures underway.

Organizational Framework for Information Security Management



Information Security Management Framework

Framework

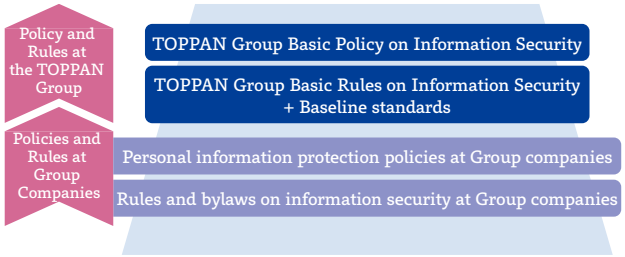
Information Security Management

Under the CISO, the Information Security Division formulates a Groupwide information security plan; sets up rules and regulations; disseminates and reviews them; convenes regular meetings with Group company members to discuss information security policies and measures underway; and carries out regular Group company audits to check the quality of security control and recommend corrective measures. The results of these activities are regularly reported to the CISO. When a security incident arises, the division promptly responds to the incident and reports the control status to the CISO, as required.

Policies and Rules for Security Governance

The TOPPAN Group Basic Policy on Information Security and the TOPPAN Group Basic Rules on Information Security comply with the ISO/IEC 27000 and JIS Q 15000 standards. Group companies formulate their own policies for personal information protection and rules and bylaws on information security in accordance with the basic policy and rules. TOPPAN's information security governance has been secured through the development of a Groupwide management framework and the dissemination of policies and rules.

Information Security Policies and Rules



Baseline Standards for Solid Security Governance

TOPPAN strives to enhance security governance by assessing the security control levels of each Group company every year according to baseline standards for evaluating conformance with the Basic Rules on Information Security. Thirty-seven items on organizational/personnel/physical elements, technical measures, incident response, and personal information protection are scored on a 5-point scale. The assessment results are reflected in the security measures of operating companies and business divisions across the Group. Improvement plans and regular progress reviews boost the quality of security control throughout the Group.

Complying with Laws and Regulations

Activity results, performance data

TOPPAN complies with laws and regulations related to privacy, confidentiality, and personal information protection in every country where the Group does business.

Japanese Personal Information Protection Act

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. Procedures are established for handling personal information and anonymously processed information, notifying individuals when their information is provided to third parties overseas, and submitting incident reports. The procedures are closely modeled after the guidelines announced by the Personal Information Protection Commission of Japan.

Overseas Legislation on Personal Information

Mindful of the importance of privacy and personal information, governments around the world are enacting laws and regulations to protect them. We take appropriate compliance measures 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

Information security systems within domestic Group companies have received PrivacyMark accreditation and information security management system (ISMS) certification. TOPPAN is formulating in-house rules, building secure environments, and training personnel in charge of information security to secure the handling of important information assets entrusted by 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 Personal Information Protection Commission. These measures cover operations involving specific personal information, such as the handling of individual identification numbers and the collection of those numbers on behalf of client companies. Dedicated rooms are set up to handle the personal identification numbers, and a special team carries out accreditation audits on their operations.

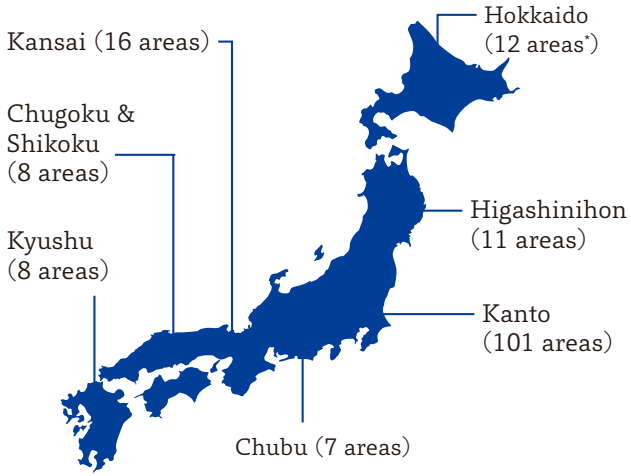
Protecting Personal and Confidential Information

Activity results, performance data

Setting up Tightly Secured Areas

Our operations involving the use of confidential materials are conducted 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 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 2023. Rigorous efforts to maintain the record of zero-incidents will continue across the TOPPAN Group.

Tightly Secured Areas in Japan (as of March 31, 2024)



*Numbers of secured areas for the handling of personal information

Controlling the Tightly Secured Areas

TOPPAN constantly upgrades security levels for the handling of personal 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. Managers assess and accredit inspection results to maintain and further enhance operational management across the Group.

Access control: Each tightly secured area is protected with technical safeguards to prevent unauthorized persons from entering (e.g., personal authentication measures, 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, entrants are prohibited from connecting any external storage media to devices used within the tightly secured areas. A two-factor authentication login system is also deployed to require the submission of an ID, password, and one or more additional factors for the use of devices in the secured areas. The monitoring center, meanwhile, operates a system to manage and analyze operational logs.

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 and confidential information are entrusted to Group and partner companies. TOPPAN also relies on the cloud services of external companies in the execution of some of the Group's 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. TOPPAN has been implementing various measures to mitigate them.

Protecting PCs and Servers with EDR App

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

Mitigating Cloud Security Risks with CSPM Service

As mega cloud services expand, we have been using a Cloud Security Posture Management (CSPM) solution to mitigate security risks in public cloud environments. The CSPM tools identify risks associated with inappropriate exposure and other settings specific to cloud configurations and promptly detect and correct any settings subject to unduly high risk.

Implementing Threat Intelligence and ASM* Service

TOPPAN continues to implement threat intelligence, third-party evaluations, and open source intelligence (OSINT) activities to detect signs of cyber-attacks against the Group and vulnerabilities visible to outside parties early on. We strive to mitigate cyber-attack risks by addressing weaknesses within the Group preemptively. We are also 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.

*Attack surface management

Upgrading Website Vulnerability Assessments

Weaknesses in our web applications have been assessed to counter cyber-attacks targeting website vulnerabilities. An automatic vulnerability detection system periodically checks the network and addresses vulnerabilities that arise from day to day. This system works synergistically with various external vulnerability-detection services to further reinforce our web-based services and our ability to provide clients with more tightly secured services. Security guidelines on coding have also been formulated for our website creators. Guideline compliance training is provided to encourage the creators to develop webpages less likely to contain vulnerabilities from the design stage.

Setting Guidelines for Cyber Emergencies

Cyber threats have been escalating across borders. Their malice and unprecedented technical cunning can result in instant and severe damage in all directions. The conventional methods used against cyber-attacks are often useless. TOPPAN formulates guidelines that summarize basic approaches, 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.

Blocking Unauthorized Connections

New safeguards are in place to mitigate the risks of virus infections and information leakages stemming from connections by unauthorized devices brought into workplaces. Our internal LAN is now equipped with network sensors. A system is also in place to check the consistency between actual in-house network communications and the IT asset information managed in our database.

Countering Email Attacks

Cyber-criminals exploit the botnet Emotet, business email compromise (BEC), and other malicious email techniques used to send fraudulent messages. As a countermeasure adopted in fiscal 2022, TOPPAN introduced 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. By providing this screening service to more Group companies from fiscal 2023 onward, we continue to fortify our email systems against cyber-attacks.

Enhancing the Capabilities of TOPPAN-CERT

TOPPAN-CERT is a cyber response team made up of specialists from across the Group. In December 2023 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) of Japan. The CERT members took the lead in responding to simulated cyber-attacks targeting the TOPPAN Group. Response procedures have been reviewed to pinpoint weaknesses in our cyber-counter capabilities and clarify improvement points in the handling of a cyber-attack. In February 2024 we established an immediate response framework to defend against cyber incidents occurring in Group companies anywhere in the world.

Sharing Information on Cyber Security Preparedness

TOPPAN holds 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.

Tightening Plant Security

Cyber-attacks continue to increase with the shift to smart factories made up of multiple network-connected components. TOPPAN is enhancing the security of facilities and equipment by familiarizing production engineers with the plant security guidelines issued in June 2023.

Acquiring Third-party Certification

Activity results, performance data

TOPPAN Group companies in Japan 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, and other third-party certifications, as shown in the following tables (as of June 30, 2024).

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

Information & Communication Division (TOPPAN Inc.); 3rd Development Department (ICT Development H.Q., Hybrid BPO Subdivision, TOPPAN Edge Inc.); Toppan Communication Products Co., Ltd.; Toppan Graphic Communications Co., Ltd.; TB Next Communications Co., Ltd.	IC23J0567
TOPPAN Edge Inc.; Information & Communication Division (TOPPAN Inc.); Toppan Communication Products Co., Ltd.; TGS Inc.	IC06J0151
Infrastructure Service Department and Service Operation Department (Service Management Center, TOPPAN Digital Inc.); DX Solution Development (ICT Development Center, TOPPAN Digital Inc.)	IC23J0568
Toppan Group Kansai Business Center (TOPPAN Edge Inc.)	JQA-IM0137
Toppan Photomask Co., Ltd.	IS 530416
ONE COMPATH Co., Ltd.	IS 533218
Security areas and ISMS Promotion Committee (Kyushu Subdivision and Chugoku & Shikoku Subdivision, Nishinihon Division, TOPPAN Inc.)	I308
Kansai Creation Division (Toppan Graphic Communications Co., Ltd.); Kansai X-tech Business Innovation Subdivision (Nishinihon Division, TOPPAN Inc.)	IC13J0361
Higashinihon Division (TOPPAN Inc.)	IS 606897
Takino Plant (Toppan Communication Products Co., Ltd.); Takino Information & Communication Engineering & Technology Team (Kansai Engineering & Technology Department, Nishinihon Division, TOPPAN Inc.)	IC14J0376
Chubu Division (TOPPAN Inc.); Chubu Production Department (Toppan Graphic Communications Co., Ltd.); Nagoya Plant (Toppan Communication Products Co., Ltd.)	IC17J0444
Service Management Group [Service desks] (System Management Department, TOPPAN Edge IT Solutions Inc.); ISO/RM Promotion Department [Administration offices] (TOPPAN Edge IT Solutions Inc.)	JUSE-IR-403
Fukuroi Plant (Toppan Forms Tokai Co., Ltd.)	JQA-IM1901
TOSCO Corp.	IC07J0211
AIOI Systems Co., Ltd.	J0265
Tokyo Shoseki Co., Ltd. [Education DX business]; EduFront Learning Research Co., Ltd.	IC23J0562
Okapi Pharmacy System Co., Ltd.	IS 794168
ORCA Management Organization Co., Ltd. [ICI Inc.]	IS 689222
One undisclosed entity	

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

Team 3 (DX Solution Development, ICT Development Center, TOPPAN Digital 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 Edge IT Solutions Inc.	10820089
TOPPAN Edge Services Inc.	10450002
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
Toppan Infomedia Co., Ltd.	24000473
livepass Inc.	25000225
Riken Genesis Co., Ltd.	14300052
booklista Co., Ltd.	10824078

Information Security Training

Training, education

TOPPAN implements extensive training and self-assessment initiatives across the Group in the belief that solidified human assets reinforce our information security management framework.

Training Employees throughout the Group

Annual training is organized to improve security capabilities of employees throughout the Group. In fiscal 2023 TOPPAN established a program entitled, "Change for a better tomorrow: Groupwide synergies to counter information security threats." The training covers comprehensive topics, from cyber-attack preparedness and daily security practices to risks specific to business divisions and compliance with Japan's amended Act on the Protection of Personal Information.

Holding Security Training for Plant Engineers

The "technical-guard training school," a program launched in fiscal 2021, aims to achieve manufacturing DX with tightly secured production sites. Trainees learn the requirements to be satisfied in deploying safeguards for the protection of manufacturing equipment during the processes from installation planning to disposal. Twenty plant engineers completed the program in fiscal 2023.

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. Results are assessed after each drill, and the challenges for senior managers are clarified to fortify their control capabilities during cyber emergencies.

Implementing Groupwide Self-assessments

We are asking every Group human asset to check their daily security practices. The 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 2023 questionnaire to confirm whether employees had appropriately updated their end-of-life software. The questions are updated each year to reinforce individual security readiness in the latest working environments.

Organizing TSAT to Elevate Security Awareness

We are strengthening our cyber defenses by enhancing the security capabilities of human assets through "TOPPAN security awareness training (TSAT)," a platform that engages trainees in a continual process of drills, evaluation, and training. Groupwide TSAT sessions have been organized regularly, and special sessions for personnel from designated departments and jobs are held whenever necessary.

Addressing Virus-infected Emails

Suspicious email reporting drills were held twice in fiscal 2023. Some 41,000 Group employees from domestic subsidiaries/associates and overseas subsidiaries took part. The participants rehearsed the procedures required for the prompt reporting of suspicious messages they had received or had already opened. The persons who opened the message were asked to take part in a follow-up program arranged to heighten their vigilance.

The drill was conducted without pre-warning. Upon receiving a fraudulent email sent out by our cyber-security team, some personnel, caught unaware, clicked a URL link to a fraudulent website.

Providing DOJO Training for Cyber Security Specialists

TOPPAN has founded Armoris Co., Ltd., a corporation 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)