Information Security Policy

Basic Policy

TAIYO YUDEN positions information security as one of the most important management issues affecting business continuity and related to maintaining and enhancing corporate value over the medium- to long-term. We established a global information security management system and promote company-wide initiatives under the Information Security Policy.

Information Security Policy

Information Security Policy

Strategy

At TAIYO YUDEN, we recognize various information assets, such as manufacturing processes, technical information, and customer information, as critical assets that are a source of competitive advantage, and we protect and manage these assets appropriately based on the level of risk.

Cyber risks, especially those affecting production sites, directly impact product quality and supply stability, thus we implement multi-layered security measures in the OT domain*, including production equipment, to strengthen the resilience of our manufacturing infrastructure.

Note: Operational Technology. Hardware and software used to monitor and control equipment and production processes in plants and other facilities.

Information Security Certification

As of June 2026, we had expanded the ISO/IEC 27001 certification acquired at our domestic Head Office and Takasaki Global Center to five sales offices in Japan and six overseas sales subsidiaries. We acquired TISAX certification at two locations, the TAIYO YUDEN Head Office and the Tamamura Plant.

Governance Structure

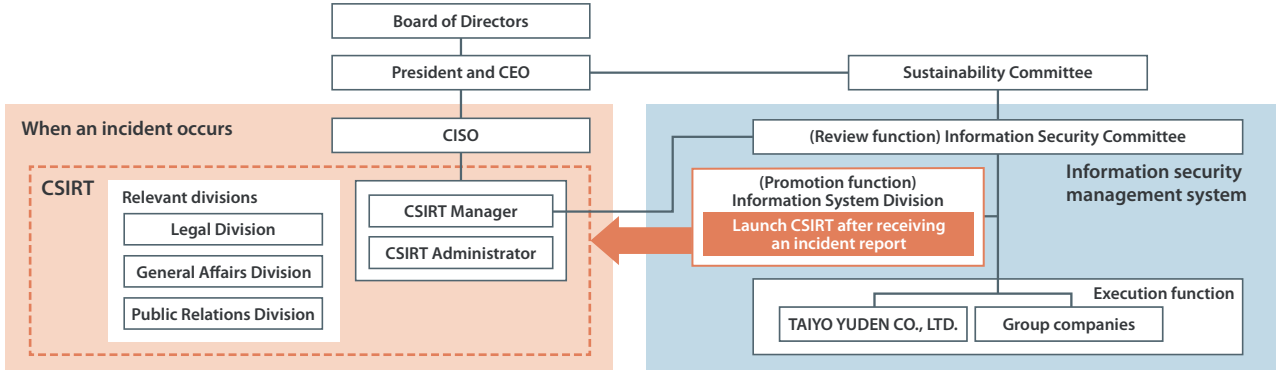
The Chief Information Security Officer (CISO) is responsible for overseeing company-wide information security measures and incident responses.

The Information Security Committee, chaired by the CISO, meets regularly to discuss the information security policy, the progress of various countermeasures, and the status of incident responses, among other matters. The details of these discussions and other key issues are reported to the Sustainability Committee twice a year and incorporated into management decision-making and oversight.

In practice, the Information System Division serves as the secretariat and promotes information security management across the Group.

Response when incidents occur

The Computer Security Incident Response Team (CSIRT) leads the initial response, ascertains the scope of impact, and implements containment and corrective measures. Incidents are promptly reported to the CISO, and when necessary, discussed by the Information Security Committee before being reported to the Sustainability Committee. As a result, we have established a system that ensures consistent decision-making and instruction, from on-site responses to management-level resolutions.



Risk Management

We continuously assess risks related to information assets and implement a multi-layered management approach combining organizational, human, physical, and technical countermeasures.

In addition to establishing group-wide regulations related to information security, we are working to improve information security literacy through training for new hires, regular training for all employees, role-based training, and suspicious email and incident response training.

In addition to controlling access to server rooms, production processes, and other critical areas, we implement integrated security measures combining defense-in-depth, measures including malware countermeasures, vulnerability countermeasures, and network security measures, with access rights management and encryption.