

Cyber Security and Data Protection

- Cyber Security
 - Policy
 - Responsible Executive and Framework
 - Information Security
 - Factory System Security
 - Product Security
 - Joint Initiative

- Data Protection
 - Policy
 - Responsible Executive and Framework
 - Personal Information Protection and Compliance
 - Responding to Incidents
 - Training

Cyber Security and Data Protection

Cyber Security

Recently, cyberattacks have become increasingly sophisticated and complex, raising the risk of large-scale incidents and damage, including attacks targeting the supply chain, such as our business partners. Simultaneously, companies are increasingly required to implement enterprise-wide cyber security measures and are expected to bear significant social responsibility in the event of security incidents.

Policy

The Panasonic Group promotes Groupwide cyber security measures to protect data and personal information entrusted to us by customers from cyberattacks and to ensure stable operations of our information systems and facilities, as well as the products and services we provide to customers.

Specifically, we have established the Panasonic Group Cyber Security Operational Rules, which apply across the Group, alongside other guidelines covering information security, factory system security, and product security, and we ensure that they are thoroughly implemented by all employees. We also regularly evaluate and review these initiatives.

Responsible Executive and Framework

The Executive Officer in charge of Cyber Security is responsible for cyber security initiatives. The Group Chief Technology Officer (Group CTO) is responsible for factory system security and product security (as of April 2026). Panasonic Holdings Corporation (“PHD”) has established the Cyber Security Supervisory Office, headed by the Executive Officer in charge of Cyber Security, to oversee the three aspects of cyber security: information security, factory system security, and product security. Through this office, we are accelerating and centralizing cyberattack countermeasures and promoting the strategic execution of cyber hygiene (prevention under normal conditions) and cyber resilience (response and recovery during incidents).

Furthermore, PHD and each operating company appoint persons responsible for information security, factory system security, and product security. Based on the basic policy and Groupwide regulations formulated by PHD, each operating company promotes security activities for each function.

The Executive Officer in charge of Cyber Security reports important matters concerning Groupwide cyber security and the status of related risks to management meetings, the Board of Directors, and other bodies. The Board of Directors supervises these matters and provides instructions and advice as necessary.

Information Security

To prevent system outages, unauthorized operation, content tampering, and other forms of damage to the Group’s internal systems, internal and external web services, and other IT systems, the Group takes a multifaceted approach to ensure that its IT systems maintain stable operations.

We build and update systems following our security policies, conduct periodic vulnerability assessments, and use periodic committee meetings and other means to ensure that IT system managers at Group companies thoroughly implement our measures.

Factory System Security

The Group has established guidelines for breach prevention, anomaly detection, and incident response covering defense against cyberattacks on its factories. We review these guidelines on an ongoing basis. All of the Group’s sites worldwide defend against cyberattack risks following these guidelines. We also conduct response training for plant personnel on the assumption that security incidents will occur, thereby raising awareness.

Product Security

As consumers conveniently use various products equipped with software and connected to networks, we must ensure product security to prevent harm from attacks initiated by malicious third parties who aim to leak or alter data or cause device malfunction. The Group has established internal structures and rules, including guidelines for promoting security-conscious development, and regularly reviews these structures and rules to ensure customer peace of mind when using products. We also promote research and development in AI-based anomaly detection technology to prevent harm from cyberattacks. Moreover, we provide training to equip employees with skills necessary to ensure product security such as risk analysis during product planning and secure coding.

Joint Initiative

To jointly tackle the above 3 initiatives, we have a dedicated team that regularly collects and monitors information about threats and vulnerabilities and implements countermeasures as necessary, while another team is dedicated to conducting drills in response to an assumed cyberattack.

Cyber Security and Data Protection

Cyber Security

- Policy
- Responsible Executive and Framework
- Information Security
- Factory System Security
- Product Security
- Joint Initiative

Data Protection

- Policy
- Responsible Executive and Framework
- Personal Information Protection and Compliance
- Responding to Incidents
- Training

Data Protection

In the course of business, companies may handle their business partners’ data assets and customers’ personal information. Improper management of such data may have a negative impact on stakeholders through information theft, leakage, and falsification. The Panasonic Group recognizes the importance of protecting personal information and other data entrusted by its business partners and customers in the course of joint research, customer service, and marketing. Accordingly, we strive to ensure information security Groupwide to prevent data leaks and data tampering.

Policy

In order to gain customer satisfaction and trust through our products and services, the Group believes it is important to recognize various types of information including personal information entrusted to us by stakeholders such as business partners and customers as important assets for these stakeholders and valuable management resources for the Group. We believe it is important to protect and handle such information appropriately. Furthermore, since the enactment of the EU General Data Protection Regulation (GDPR), personal information protection legislation has been enacted and/or revised in various countries, and its importance is growing as our Group’s data utilization businesses expand.

Therefore, we are committed to ensuring information security and protecting personal information under a unified Groupwide framework and in accordance with the information security policies outlined in the Panasonic Group Code of Ethics and Compliance, as well as management regulations and guidelines related to information security, and the basic information security and personal information protection policies established by all Group companies.

We ensure transparency in the handling of personal information by providing timely notice or disclosures to users of our products and services or individuals who are the subjects of personal information regarding our purposes for using personal information and other relevant matters and any updates of our policies, as required by applicable laws and regulations, and depending on individual circumstances. We implement the appropriate organizational, technical, and physical security management measures to accurately record information; properly manage, use, and dispose of it; and prevent its unauthorized use, leakage, and falsification. We set limits on retention periods for personal information, depending on the purpose for which the information is acquired and as required by law. We also strive to raise employee awareness through regular employee training, confirm and evaluate the state of our information handling through internal audits, and make improvements as needed. These initiatives are evaluated and reviewed periodically in light of changes in laws and regulations, changes in the business environment, as well as incidents and audit results.

We have established systems to respond to requests from individuals regarding the disclosure, correction, or deletion of their personal information, as well as concerns or complaints related

to personal information (privacy). We notify or publish the contact point for inquiries in a manner that is easy for individuals to understand and access.

Furthermore, we ensure that information provided to third parties is protected at a level consistent with the Group's policies by taking all necessary and appropriate measures, including ensuring that they are adequately managed and contracts are signed to ensure that third parties appropriately manage the information provided to them.

[🔗](https://holdings.panasonic/global/corporate/about/code-of-conduct.html) **Panasonic Group Code of Ethics & Compliance “Protecting and using our company assets (Information Security)”, “Respecting individuals’ privacy”**
<https://holdings.panasonic/global/corporate/about/code-of-conduct.html>

[🔗](https://holdings.panasonic/global/security-policy.html) **Basic Information Security Policy (an example of PHD)**
<https://holdings.panasonic/global/security-policy.html>

Responsible Executive and Framework

The Executive Officer in charge of Cyber Security is responsible for information security and the protection of personal information (as of April 2026).

The Group has appointed persons responsible for information security and personal information protection at PHD and each operating company, and each operating company promotes information security initiatives in line with the Basic Information Security Policy and Global Rules established by PHD.

The Executive Officer in charge of Cyber Security reports important matters and the status of risks related to information security and the protection of personal information (privacy) across the Group to management meetings, the Board of Directors, and other bodies. The Board of Directors supervises these matters and provides instructions and advice as necessary.

[🔗](https://holdings.panasonic/global/corporate/sustainability/governance/security/iso27001.html) **List of ISO27001 certified companies in Panasonic Group in Japan**
<https://holdings.panasonic/global/corporate/sustainability/governance/security/iso27001.html>

Personal Information Protection and Compliance

In recent years, many countries have enacted or revised personal information protection laws and regulations. We recognize the importance of ensuring thorough compliance with personal information protection laws and regulations.

As our IoT business grows, our employees are increasingly likely to handle customer life-log data and other personal information worldwide. Therefore, the Group is striving to improve its data management to provide a higher level of privacy protection. Additionally, to comply with the EU General Data Protection Regulation (GDPR), and other laws in various countries, we have developed response manuals and are strengthening our efforts to ensure compliance and accountability to society through employee education and other initiatives. The Group strives to

Cyber Security and Data Protection

Cyber Security

- Policy
- Responsible Executive and Framework
- Information Security
- Factory System Security
- Product Security
- Joint Initiative

Data Protection

- Policy
- Responsible Executive and Framework
- Personal Information Protection and Compliance
- Responding to Incidents
- Training

protect personal information based on the Personal Information Protection Policy established by each Group company, which mirrors PHD’s policies.

In addition, we are responding to risks by classifying personal information according to its sensitivity and the impact of its disclosure, and then implementing organizational, technical, and physical security control measures depending on that classification. We have mechanisms in place to verify how personal information is handled across the Group, and regularly assess risks related to personal information (privacy).

Example: PHD

 **Panasonic Information Protection Policy**

<https://holdings.panasonic/global/privacy-policy.html>

 **Public information and requests for disclosure of personal information based on the “Personal Information Protection Law”. (Japanese only)**

<https://holdings.panasonic/jp/privacy-policy/public-announcement.html>

Responding to Incidents

The Group has established reporting and response systems in its incident response rules and provides thorough training employees to minimize harm in an event of an incident. In the unlikely event of an incident, we also work to identify the causes and prevent recurrence. We have established internal procedures and systems to ensure that notifications to the individuals concerned and reporting to supervisory authorities can be carried out appropriately.

Training

The Group conducts annual information security and personal information protection (privacy) training to raise each employee’s security awareness and promote behavioral change. Using content tailored to each employee’s needs (level-specific for newly hired or promoted employees, or company-wide training), we carry out training on appropriate information management and cyber security along with drills to respond to targeted attacks.

■ FY2026 Groupwide training achievements

Information Security:

- Training content: Enforcing information security and personal information protection
- Target trainees: All employees of Panasonic Group subsidiaries and affiliated companies

Cyber Security:

- Training content: Cyber security training and drills
- Target trainees: All employees of Panasonic Group subsidiaries and affiliated companies