Cyber Security and Data Protection

Cyber Security

Recently, cyberattacks have become increasingly sophisticated and creative, raising the risk of large-scale incidents and damage, including targeting our business partners and supply chains. Simultaneously, companies must deploy enterprise cyber security measures, as society demands responsibility for addressing security incidents.

Policy

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

Specifically, we established the Panasonic Group Cyber Security Operational Rules that apply across the Group alongside other guidelines all employees must follow involving information security, manufacturing system security, and product security. We also regularly evaluate and review these initiatives.

Responsible Executive and Framework

The executive officer responsible for cyber security is the Group Chief Information Officer (Group CIO). The Group Chief Technology Officer (Group CTO) is responsible for manufacturing system and product security. (as of August 2023)

Panasonic Holdings Corporation (PHD) established the Cyber Security Supervisory Office, headed by the Group CIO, to oversee the three aspects of information, manufacturing system, and product security, accelerate and focus cyberattack countermeasures, and promote cyber hygiene (prevention under normal conditions) and cyber resilience (response and recovery during incidents).

Furthermore, PHD and our Group companies appoint managers in charge of information security, manufacturing system security, and product security. All Group companies promote security strategies for all functions based on PHD's basic policy and Groupwide regulations.

Major Initiatives

Information Security

To mitigate stoppages, unauthorized operation, content falsification, and other damage to the Group's internal systems, internal and external web services, and other IT systems, Panasonic takes a multifaceted approach to ensure that our IT systems maintain stable operations. We build and update systems following our security policies, conduct periodic vulnerability assessments, and provide IT system managers at Group companies with thorough strategies to follow through periodic committee meetings and other means.

Manufacturing System Security

Panasonic 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 Panasonic'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 to help raise awareness.

Product Security

As consumers use various software-driven products through convenient network connections, 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. Panasonic establishes internal systems and rules, including guidelines for promoting security-conscious development. It regularly reviews these systems 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, there are training to provide employees skills necessary to ensure product security such as, risk analysis and secure coding, etc.

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 harm stakeholders, including information theft, leakage, and falsification. Panasonic Group is well aware of the importance of protecting personal information and other data entrusted by its business partners and customers through joint research, customer service, and marketing. Thus, we strive to ensure information security Groupwide to prevent data leaks and data tampering.

Policy

Earning the trust and satisfaction of our customers with our products and services is at the core of our management philosophy. In line with this goal, we recognize that the information and personal information we receive from our customers and other stakeholders are significant assets to everyone involved and valuable management resources to Panasonic. Therefore, we believe we must adequately protect and handle this information. Additionally, to comply with the EU General Data Protection Regulation (GDPR), and other laws in various countries, we have prepared response manuals and are strengthening our efforts to ensure compliance and accountability to society through employee education and other measures.

Therefore, based on the Panasonic Group Code of Ethics & Compliance, which includes information security policies, management rules and guidelines related to information security, and the Basic Information Security Policy and Personal Information Protection Policy established by each Group company, we strive to ensure security and protect personal information. By implementing organizational, technical, and physical security management measures, we accurately record information; properly manage, use, and dispose of it; and prevent its theft, leakage, and falsification. Additionally, we periodically conduct awareness building activities as part of our employee training, and evaluate how we handle information, review it, and implement improvement through internal audits.

We also take necessary and appropriate measures, including thorough management and contract execution, to ensure that contractors properly manage security for the information we provide to them.

WEB **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

WEB **Basic Information Security Policy (an example of Panasonic Holdings Corporation)**
https://holdings.panasonic/global/security-policy.html

Responsible Executive and Framework

The executive officer in charge of information security and protection of personal information is Group Chief Information Officer (Group CIO) (as of August 2023).
Panasonic Group has established responsible person in charge of information security and personal information protection in PHD and each Operating Company, and each Operating Company promotes information security initiatives in line with the Basic Information Security Policy, established by PHD.

WEB **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 thorough compliance with personal information protection.

As our IoT business grows, its employees are increasingly likely to handle customer lifelogs and other personal information worldwide. Therefore, Panasonic 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 prepared response manuals and are strengthening our efforts to ensure compliance and accountability to society through employee education and other measures.

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

Ex.) Panasonic Holdings Corporation

WEB **Panasonic Information Protection Policy**
https://holdings.panasonic/global/privacy-policy.html

WEB **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

Panasonic has established reporting and response systems in its incident response rules and thoroughly trains employees to minimize harm during an incident. In the unlikely event of an incident, we also work to uncover the cause and prevent recurrence.

Training

At Panasonic, we conduct appropriate information management training and targeted attack drills for all employees to raise their awareness and knowledge so they can manage information properly. We provide information security training according to each employee's needs, including training by organizational level (upon beginning employment, when promoted, and so on) and training for those who directly handle personal information and other information with which the company has been entrusted.

FY2023 Groupwide training achievements

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