Social — Data Security

Policy

The KWE Group handles customer, personal, and business-related information during the conduct of business and established the KWE Group Information Security Basic Policy in 2007. In 2020 the KWE Group established the KWE Group IT Security Policy conforming to the ISO 27001 standard to improve the security management framework.

KWE Group Basic Policy on Information Security

KWE Group will run our business operations successfully and continuously improve information security in order to increase stakeholders' trust, while maintaining confidentiality, integrity, and availability of information assets. Our Basic Policy includes the following:

1. Build organizational structures to improve our information security
2. Comply with all information security laws, regulations, and other internal rules
3. Regularly evaluate and re-examine measures for information security
4. Reliably protect information assets against threats (unauthorized access, computer viruses, etc.)
5. Take measures aimed at enabling the rapid recovery of business activities from setbacks and natural disasters

KWE Group IT Security Policy

Summary

- Establishing appropriate local IT security policy, planning, and governance
- Implementing appropriate security controls
- Regularly reviewing the suitability, adequacy, and effectiveness of the security controls
- Improving the suitability, adequacy, and effectiveness of the security controls

Creating Corporate Value

For the material topic Data Security, the KWE Group continues to improve information technology security in order to address threats that are becoming increasingly more sophisticated.

After establishing the KWE Group IT Security Policy in 2020, in 2021 we assessed security levels, built a security management framework, and began employee education and training. In 2022, we focused on standardizing our IT infrastructure and implementing periodic assessments.

We are moving forward on building a zero trust security platform, utilizing services that can guarantee security in the cloud, and educating users including employees and business partners.

Also, under the important theme of improving security across the KWE Group, we are performing security assessments of our data center, server, and network environments.

We will continue to take swift and appropriate action to improve information technology security, remain a trusted business partner for our stakeholders, reduce potential impediments to future growth, and thereby drive the KWE Group's sustainable growth and create corporate value.

Cybersecurity Measures

We install and implement hardware and software cybersecurity including entrance control, exit control, and vulnerability prevention measures. In addition to server management, we always monitor potential security anomalies 24/365, with prompt discovery and corrective action in the event of an incident.

Based on the circumstances and details of the server failure that occurred within our systems in April–May 2025, we have defined the following key measures to prevent recurrence:

1. Improve security governance
2. Implement measures against emerging threats
3. Prevent the spread of damage by consolidating networks
4. Ensure business continuity by improving disaster resistance

Employee Education

E-learning for employees on information security was held four times in FY2024. And in light of the increasing number of cyber-attacks via email and the risk of fake news created by generative AI, phishing email drills were held twice as well.

Employee Education (FY2024)

When	Content
April - June 2024	Representative threats in 2024
July - September 2024	Social engineering and multi-factor authentication
October - December 2024	How to use the phishing alert button
January - March 2025	Security awareness training by Kevin Mitnick (2024)

Periodic Security Assessments

KWE Group data security undergoes regular third-party assessments, with any required improvements planned and implemented by information security experts.

Other Risk Reduction Measures

We use decentralized data centers, cloud resources, and redundant network lines to minimize cybersecurity risks and ensure availability. Each Group company's outward facing servers undergo vulnerability scans to reduce the risk of breach of confidential information. We are also implementing functions that use AI and big data to counter malware and spam email, and KWE uses automated processes to speedily deal with threats that are detected. We are adding scenarios to the Microsoft 365 chatbot to assist users in identifying suspicious email. This helps prevent security incidents by enabling employees to use the chatbot to decide what to do with suspicious emails in a timely manner.