Material Topics

Data Security

Objectives	Progress in FY2023	FY2024 Onward
■ Improve information security architecture ■ Increase employee awareness of information security	■ Elearning for all KWE Group employees was held four times ■ Phishing email drills were held 5 times ■ Expanded employee training in cyber-security and conducted periodic security assessments ■ Improved security assessment of data center, server, and network environments under the Unus Project to establish a group-wide IT platform and improve security across the group ■ Improved measures for suspicious emails, in addition to existing malware and spam email measures	■ Implement regular third-party assessments, with improvements planned and implemented by information security experts ■ Continue fast and effective measures to improve IT security ■ Utilize generative AI to improve competitive advantage and operations efficiency, and build framework to improve risk management

Diversity and Equal Opportunity

Objectives	Progress in FY2023	FY2024 Onward
■ Promote equal opportunity in promotion to management ■ Promote hiring from minority groups ■ Promote educating employees about human rights and equal opportunity	■ Started employee engagement surveys ■ Women in management positions across the group 34.0% ■ Educated employees about human rights and equal opportunity though elearning ■ Expanded frameworks for telework and reduced work hours for child care	■ Increase employee awareness of KWE Group Diversity and Equal Opportunity Policy ■ Move ahead on activity in line with local characteristics

Social Impacts in the Supply Chain

Objectives	Progress in FY2023	FY2024 Onward
■ Fulfill supply chain ethical, social, and environmental responsibilities	■ Moved ahead on establishing unified supplier safety and health standards ■ Participated as KWE Group in the UN Global Compact ■ Participated in Partnership Building Declaration ■ Established Human Rights Due Diligence Committee	■ Move ahead on the KWE Group Human Rights Policy ■ Move ahead on supplier survey with a checklist including human rights due diligence

Data Security

Concept & 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

Progress

The KWE Group continues to improve IT security in order to address the threats becoming increasingly more sophisticated with accelerating change in the business environment.

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.

In March 2023 we started up the Unus Project to establish a group-wide IT platform. Under the important theme of improving security across the group, we are performing security assessments of our data center, server, and network environments.

We will continue taking fast and effective measures to improve IT security in order to be a reliable business partner for our stakeholders, and contribute to the ongoing growth of the KWE Group.

Cyber-security

We install and implement hardware and software cyber-security 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.

Employee Education

E-learning for employees on information security was held four times in FY2023. 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 five times as well.

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 cyber security 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. In October 2023 we added 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.

Employee Education (FY2023 on)

When	Content
June - July 2023	Phishing email drills
July - August 2023	Information security e-learning
August 2023	Phishing email drills
September - October 2023	Phishing email drills
October 2023	Information security e-learning
December 2023	Phishing email drills
	Information security e-learning
February 2024	Phishing email drills
March 2024	Information security e-learning