

Material Topics

Data Security



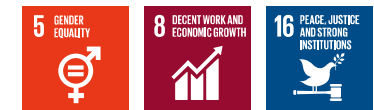
Objectives	Progresses in FY2022	FY2023 Onward
<ul style="list-style-type: none"> Improve information security architecture Increase employee awareness of information security 	<ul style="list-style-type: none"> Implemented cyber-security measures Periodic security assessments by a third-party Reduced data center, server, and network risks Educated and trained employees (phishing email drills and security training, each three times a year) 	<ul style="list-style-type: none"> Implementing cyber-security measures Periodic security assessments by a third-party Reducing data center, server, and network risks Educating and training employees (phishing email drills and security training, each four times a year)

Diversity and Equal Opportunity



Objectives	Progresses in FY2022	FY2023 Onward
<ul style="list-style-type: none"> Promote equal opportunity in promotion to management Promote hiring from minority groups Promote educating employees about human rights and equal opportunity 	<ul style="list-style-type: none"> Women in management positions across the Group: 34.3% Educated employees about human rights and equal opportunity through e-learning 	<ul style="list-style-type: none"> Establishing KWE Group Diversity and Equal Opportunity Policy Moving ahead on activity in line with local characteristics

Social Impacts in the Supply Chain



Objectives	Progresses in FY2022	FY2023 Onward
<ul style="list-style-type: none"> Fulfill supply chain ethical, social, and environmental responsibilities 	<ul style="list-style-type: none"> Assessed procurement and identified priority areas (occupational safety and health, labor, vendor management, and environmental compliance) Occupational safety and health checklist (37 items in 7 areas) 	<ul style="list-style-type: none"> Providing checklist to suppliers and do survey Supplier management framework

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 is committed to ongoing improvement of our information security to maintain the confidence of our customers, business partners, and other stakeholders.

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.

The business environment continues to change rapidly, and threats to corporate IT security are becoming more clever and more advanced. Appropriate and timely measures must be exercised on an ongoing basis.

Specifically, we are moving forward and building a zero trust security platform, utilizing services that can guarantee security in the cloud, and educating users such as employees and business partners about how to counter threats.

IT security remains an important area to be addressed, and it is critical to the sustainability of the KWE Group and its stakeholders.



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 three times in FY2022. Considering the rising trends in phishing emails, drills were held three times in FY2022 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.

Employee Education (FY2022 on)

When	Content
June - July 2022	Phishing email drills: All sites (10,765 employees) Information security e-learning
November - December 2022	Phishing email drills: All sites (11,994 employees) Information security e-learning
February - March 2023	Phishing email drills: All sites (12,363 employees) Information security e-learning

