Emerging Risk Management

The company continuously monitors external trends and conditions, recognizing the importance of emerging risks that may impact the business in the short, medium, and long term. The company can proactively implement measures to prevent these risks in advance and create growth opportunities for the business.

Emerging Risk Issues	Details	Impact (Positive/Negative).	Risk Mitigation Measures
1. Climate change risks leading to more frequent and severe natural disasters.	Extreme weather conditions cause natural disasters such as sea-level rise, land subsidence, severe flooding, extreme drought, and heatwave damage.	☞ Competitive advantage in the tap water business increases. ☞ Sanitation, safety, and protection of life and property decrease. ☞ Business continuity management costs increase. ☞ Business continuity may be disrupted.	☞ Set organizational greenhouse gas reduction targets to achieve net-zero emissions by 2050. ☞ Closely monitor climate change developments and updates from relevant agencies. ☞ Control tap water production to comply with environmental standards (ISO 14001). ☞ Regularly conduct natural disaster emergency drills and update plans to stay aligned with current conditions. ☞ Strictly comply with environmental laws and regulations.
2. Risks in transitioning to a low-carbon economy due to uncertainties in policies and international regulatory standards.	The low-carbon economy leads to the implementation of greenhouse gas emissions trading systems (ETS), carbon taxes, cross-border carbon adjustment measures (CBAM), and carbon credit systems.	☞ Competitive advantage in the tap water business increases. ☞ Costs of managing the low-carbon economy increase. ☞ Food and water security decreases.	☞ Set organizational greenhouse gas reduction targets to achieve net-zero emissions by **2050.** ☞ Closely monitor climate change updates and developments from relevant agencies. ☞ Ensure tap water production complies with environmental standards (ISO 14001).
3. Risks from geopolitical conflicts, war, and geoeconomic confrontations.	Rising geopolitical risks are expected to lead to a multipolar world. In the past, the United States was the sole power shaping the global order. Currently, emerging major powers such as China, which is increasingly influencing the global economy, and Russia, which plays a key role in the global energy sector, are gaining significant influence.	☞ Increased trade or business restrictions from major powers. ☞ Food and water security declines.	☞ Closely monitor geopolitical conflicts, war, and geoeconomic confrontations through updates from relevant agencies. ☞ Adjust emergency plans to address risks from war or geopolitical threats.

Emerging Risk Issues	Details	Impact (Positive/Negative).	Risk Mitigation Measures
4. Cybersecurity risks to information security arising from evolving forms of cyberattacks.	☞ Cyber threats are becoming increasingly complex and sophisticated. Attacks do not always target organizations directly; instead, cybercriminals often exploit software or services used by the organization. This is known as a "Supply Chain Attack" turning trusted software into a weapon against the organization's own systems. ☞ AI-driven ransomware is making cyberattacks faster, smarter, and more difficult to detect and prevent.	☞ Evolving cyberattack techniques can cause significant business disruption and increase the risk of data breaches or unauthorized disclosure of the Company's and stakeholders' personal information more rapidly and easily. ☞ Confidence in the Company's ability to maintain the security of its information technology systems may decline. ☞ Organizational costs may increase due to penalties, compensation, and remediation expenses. ☞ Disputes or complaints may arise between the Company and its stakeholders, such as employees, customers, and business partners, regarding data breaches or violations of personal data privacy.	☞ Communicate the information and cybersecurity policy to executives and employees as operational guidelines. ☞ Strictly enforce compliance with information technology security policies and practices. ☞ Strictly comply with the Information Security Control Procedures Manual. ☞ Strictly implement the IT Disaster Recovery and Cybersecurity Incident Response Plan in cases of system breaches and cyber threats, and regularly update the plan to address evolving situations. ☞ Promote and communicate information to raise awareness of information technology security among the Company's personnel.