Information Security and Privacy Protection Policy of BEWG

Article 1 Background

In the era of digitalization and intelligent transformation, information security and privacy protection have become essential pillars of sustainable enterprise development. As a leading environmental water-services company, BEWG is committed to building a secure operating network and safeguarding the information and privacy rights of both users and the Group. This Policy is therefore enacted to strengthen Group-wide information security and privacy protection.

Article 2 Scope of Application

This Policy applies to all Group employees and third parties (e.g., suppliers). Overseas operations should comply with local laws and regulations under the guidance of this policy.

Article 3 Governance Structure

The Group has established a three-tier information security governance structure consisting of executive, management and execution, and continues to improve the management responsibilities of information security at each level.

1. Executive: Information Security Leadership Team is responsible for coordinating the overall strategic planning of the Group's information security; Making decisions on major issues related to the information security of the Group; Reviewing and monitoring the information security within the Group; Coordinating and promoting the daily information security work of the Group.
2. Management: Information Security Management Team is responsible for daily management of the information security, implementation of the information security planned by the information security leadership team, overall maintenance and continuous optimisation of the information security; Provide professional support and guidance for the information security of the Group; Responsible for the Group's information security risk assessment; Organise the supervision and inspection of the Group's information security. Responsible for handling the reporting and inquiries of employees regarding privacy protection issues or concerns.
3. Execution: Consist of Enterprise Digital Centre, information security specialists from all centers, regions and business units. Enterprise Digital Centre is responsible for implementing the Group's information security policies and objectives, develop future plans for information security construction, and continue to carry out information security construction of the Group. Information security specialists are responsible for cooperating with the information security management team to complete work related to information security, such as communication and tracking on implementation of security system requirements, coordination and promotion of

continuous management of information assets in the department, timely reporting of security incidents and cooperation in response, etc.

Article 4 Management Mechanisms

1. All employees of the Group shall bear the responsibility of protecting information security and customer privacy. They must strictly comply with relevant systems, proactively prevent data leakage risks throughout the business process, and ensure compliance with operational requirements. We have established a punishment mechanism to impose disciplinary actions such as warnings, criticism, and dismissal on employees who violate the Group's information security and privacy protection requirements.

2. In terms of the user data collected and involved in business operations, the Group commits to ensuring the integrity of the data and providing protection. We have incorporated relevant policies and procedures into the Group's compliance operation management system and initially established a user privacy data protection mechanism in accordance with internal requirements. We implement strict data classification measures to prevent unauthorized access, tampering or destruction. At present, the Group has standardized the management of user data collection, use, storage and destruction through measures such as access control, third-party management and incident response.

3. In terms of information security management, the Group is committed to actively monitoring cyber security risks, promptly implementing response measures for emergencies, efficiently dealing with information security threats, and continuously enhancing the security and stability of information systems. We regularly complete the annual review of ISO 27001 Information Security Management System certification, monitor network security risks and conduct network emergency event drills. We provide information security training for all employees to make each one aware of the importance of information protection and data security.

4. In terms of external third-party cooperation, we have formulated and released the *Supplier Information Security Management Regulations of BEWG*, which standardizes the principles and requirements for the information security management of suppliers of BEWG, strengthens and standardizes the information security management of suppliers, and minimizes the information security risks introduced by suppliers.

Article 5 Annex

1. The Group will periodically review the implementation of this Policy and update it in line with applicable laws and changing circumstances.

2. This Policy takes effect on the date of publication.