Attachment No. 9

Data Protection Policy
(In accordance with the Personal Data Protection Act B.E. 2562)

Millennium Group Corporation (Asia) Public Company Limited (the "Company") recognizes the importance of personal data protection and operates in compliance with the Personal Data Protection Act B.E. 2562 and all relevant regulations, ministerial rules, and notifications that may be issued in the future (collectively referred to as the "Personal Data Protection Laws").

The Group Chief Executive Officer has enforced the Company's Data Protection Policy across the Company and its subsidiaries to establish guidelines for managing and safeguarding personal data that is collected, used, or disclosed by the Company and its subsidiaries in accordance with applicable laws. The key elements of this Policy are as follows:

1. Directors, executives, employees (both permanent and temporary) of the Company and its subsidiaries must strictly comply with the applicable laws, policies, regulations, manuals, or practices related to personal data protection.
2. Directors and executives at all levels must promote awareness of personal data protection among employees and encourage risk management practices across all organizational levels. Effective internal controls must be established to prevent unauthorized collection, use, or disclosure of personal data.
3. The Company shall appoint a Head of the Personal Data Protection Unit (Head of PRC), responsible for advising, monitoring, and ensuring that personal data handling complies with relevant laws. The Head of PRC shall also coordinate with and support the Personal Data Protection Committee. Directors and executives must support the Head of PRC by providing adequate resources and access to personal data.
4. Personal data shall be collected only as necessary and for lawful purposes related to the Company's processing activities.
5. The collection, use, or disclosure of personal data must be based on explicit consent from the data subject and must be accompanied by sufficient information provided to the data subject before or at the time of data collection, as required by law.
6. Personal data must be used only for the stated purposes given to the data subject at the time of collection unless otherwise permitted by law. Collection from third-party sources must also be disclosed and consented to unless exempted by law.
7. The Company and its subsidiaries must maintain and regularly update a Record of Processing Activities (ROPA) to allow access and review by the data subject or the Office of the Personal Data Protection Committee.
8. Adequate security measures must be in place to protect personal data from loss, unauthorized access, alteration, or disclosure. These measures must be reviewed regularly or whenever necessary, including in response to technological changes.

9. The Company and its subsidiaries must implement a process to delete or destroy personal data once the retention period has ended or when data becomes irrelevant or excessive unless retention is required by law.

10. Where a data processor is engaged, the Company or its subsidiaries must enter into a data processing agreement to ensure compliance with the law and prevent misuse or unlawful disclosure of personal data. Ongoing monitoring of the processor's compliance is required.

11. When disclosing personal data to external parties (e.g., regulators, law enforcement, insurance providers), the Company must ensure proper consent has been obtained unless the disclosure falls under lawful exceptions (e.g., legal obligations, vital interests, or legal claims). Disclosure records must be maintained.

12. If personal data is to be transferred internationally, the Company must ensure the destination country has adequate data protection standards or that a Data Transfer Agreement is in place, as required by law.

13. Directors, executives, employees, and contractors must report any personal data breach to the Office of the Personal Data Protection Committee within the required timeframe and notify the data subject without delay if the breach is likely to affect their rights and freedoms, unless the risk is minimal.

14. All personnel must cooperate with the Head of PRC and the regulatory authority by providing documents or information upon request and support any investigations or compliance reviews.

15. The Company will provide regular training and awareness programs to all employees to strengthen compliance with personal data protection laws and build an organization-wide culture of data privacy awareness.