



Confidentiality and Personal Data Protection Policy

Bags and Gloves Co., Ltd.

Effective Date: 9 April 2025

1. Purpose of the Policy

This Policy is established to provide guidelines for the control and management of the storage, use, and disclosure of the Company's confidential information as well as personal data as defined under the Personal Data Protection Act B.E. 2562 (PDPA), with the following objectives:

1. Not to disclose or use confidential or personal data for purposes unrelated to work or the relationship with the Company, or without the Company's prior written consent.
2. To ensure that the Company, its employees, and related parties restrict access to data only on a need-to-know basis.
3. To implement appropriate measures to prevent data leakage.
4. To notify the Company immediately upon suspicion of a potential data breach.
5. To return or destroy confidential and personal data immediately upon termination of the relationship or upon the Company's request.
6. The Company reserves the right to enforce these obligations directly against outsourced personnel. In the case of engagement through third-party entities, this Policy shall form part of and be binding in conjunction with the principal contractual agreement.

The provisions herein serve to ensure that the handling of confidential and personal data complies with the PDPA.



2. Scope of the Policy

This Policy applies to:

- All levels of employees, shareholders, independent contractors (freelancers), interns, consultants, external service providers (outsourcing), business partners, clients, service users, business negotiators, and any individuals or entities to whom the Company discloses information during business operations, including their employees and representatives.

3. Definitions

- **Company Confidential Information:** Information related to the Company's business in any form (documentary, digital, or verbal) not disclosed to the public, including but not limited to business plans, marketing strategies, production formulas, development processes, product data, software, source code, customer/partner/supplier information, password, financial records, contracts, legal documents, internal reports, and policies.
- **Personal Data:** Any information, whether in documentary, written, or digital form, that can directly or indirectly identify a person, such as name, national ID number, address, phone number, email, health information, IP address, nationality, race, religion, beliefs, political opinions, etc.
- **Data Recipient:** Any employee, individual, or legal entity who receives, accesses, or handles the Company's confidential or personal data, by any means.

4. Guidelines for Protecting Confidential and Personal Data within the Company

All Data Recipients must comply with the following guidelines:

4.1 Limited Use

- Use data only as necessary for the purpose of the assigned task or



contractual obligation.

- Do not use data for any other purpose or for personal or third-party benefit.

4.2 Access Control

- Limit access strictly to those who need to know, and store data in secure rooms, cabinets, or protected digital storage with access control measures.
- Do not transmit, sell, transfer, or share any data with unauthorized persons by any means.

4.3 Preventing Data Breach

- Store data in secure locations and digital systems, employing encryption, strong passwords, and cybersecurity protocols.
- Do not record or transmit confidential information via uncontrolled channels such as personal emails, Line, personal cloud storage, or any other unregulated platforms.
- Retain data only for the necessary duration of use.
- Properly destroy or delete data when no longer needed.

4.4 Incident Notification

- In case of suspected data or confidentiality breach, the Recipient must immediately inform the Company.
- The Company has the right to investigate and take disciplinary or legal actions as appropriate.

4.5 Data Return or Destruction

- Upon termination of the relationship, the Company may request the immediate return, deletion, or destruction of confidential and personal data.
 - The Recipient must confirm destruction according to the method prescribed by the Company.
-



5. Compliance with PDPA and Data Subject Rights

The Company respects the rights of data subjects under the PDPA, including the rights to:

- Access, correct, delete, restrict processing, or withdraw consent;
- Object to data processing;
- File complaints with the Personal Data Protection Committee (PDPC).

All data processing shall be conducted under a lawful basis such as consent or the legitimate interest of the Company, as applicable.

6. Violations and Penalties

Any violation of this Policy is considered a serious offense. The Company reserves the right to take the following actions:

- Disciplinary measures for employees;
 - Termination of contracts or suspension of payments for contractors or external parties;
 - Legal action for civil damages;
 - Filing of criminal charges (in cases of severe violations under the PDPA or trade secret laws).
-

7. Policy Review and Amendments

The Company reserves the right to revise this Policy as appropriate or when required by legal changes. Any amendments shall be communicated to the relevant parties in advance.



8. Acceptance of the Policy

Any Data Recipient assigned to perform duties or having a business relationship with the Company shall be deemed to have accepted and agreed to fully comply with this Policy.

Issued by
Bags and Gloves Co., Ltd.

Signed:

(.....Jitanan Sitthi-Ampai.....)

Managing Director

Date:**9 April 2025**.....