Personal Data Protection Policy
For Employee of Carabao Group Public Company Limited and Subsidiaries

Carabao Group Public Company Limited and its subsidiaries **("the Companies")** recognize the importance of protection for your personal data under the Personal Data Protection Act of B.E. 2562 (including revisions) **("the Act")**. Therefore, the Companies have publicized this personal data protection policy **("the Policy")**. The objective of the collection, use and/or disclosure of your personal data as job applicants, current employees, former employees, contractors, executives, directors, shareholders, family members, references or any other ordinary persons involved (collectively known as **"you"** or **"the employee"**). The Companies recognize your importance as the Companies' employee. This policy elaborates the process for personal data protection and provides guidelines for properly handing data in compliance with the Act.

1. Personal Data Collected, Used and/or Disclosed by the Companies

"Personal data" means data concerning ordinary persons that can identify the person directly or indirectly as specified below.

"Sensitive personal data" means personal data categorized as sensitive personal data as specified below.

"Personal data collected, used and/or disclosed by the Companies" means data concerning you collected by the Companies and affiliated companies (as specified in Clause 5). The aforementioned data collection depends on the relationship between the Companies and you. The types of personal data collected by the Companies are as follows:

1.1 Your Personal Data

Your personal data collected, used and/or disclosed by the Companies includes and is not limited to the following personal data:

1) **Personal data** such as first names-last names, titles, nicknames, gender, date of birth, age, identification data issued by the government (such as identification numbers, passport numbers, driver's license numbers), marital status, military status, photographs, age, place of birth, blood type and/or citizenship.

2) **Contact data** such as addresses, telephone numbers and/or email.

3) **Financial data** such as monthly salaries, remuneration, bank account numbers and/or other compensation.

4) **Personal and experience background data** such as educational backgrounds, internship program, skill and expertise training backgrounds, work experience/history backgrounds.

5) **Working experience data** such as job positions, work permits, your working experience data, performance assessment data, working performance, history of leave and/or data concerning use of the Companies' information systems and internal websites.

6) **Data from video or audio recordings during work** such as closed-circuit television camera data and/or audio recordings of conversations when communicating with outside customers or persons or at meetings based on positions and duties. For closed-circuit television camera data, please see the details on collection, use and/or disclosure of data from the Companies' closed circuit television cameras under the "Personal Data Protecting Policy for the Use of Closed-circuit Television Cameras" at https://investor.carabaogroup.com/en/corporate-governance/corporate-governance-policy-and-others

7) **Other personal data** such as any personal data of person, who perform in obligation connecting with you, provided for the company with consent or the company received such of personal data from other person or the related agency and/or

8) **Sensitive personal data** such as health data (history of illnesses and treatment), criminal backgrounds and/or biological data with obtaining your consent or necessary permitted by law.

1.2 Personal Data of Third Parties

If you provided the personal data of third parties (such as family members, guarantors (if any) and references) for the Companies or if you required the Companies to disclose personal data of third parties to the outside persons, you have the duty to notify the aforementioned third parties of details in this policy regarding to require for consent from the aforementioned persons (in cases where consent is required). You may check the accuracy and completeness of personal data and inform the Companies of change matters in such of personal data. Furthermore, you have the duty to enable the Company to collect, use and/or disclose personal data of the aforementioned persons pursuant to the law and prescribed in this policy.

1.3 Personal Data of Youths, Quasi-incompetent Persons and Incompetent Persons

In some cases, prescribed by law, the Companies may not collect, use and/or disclose the personal data of youths, quasi-incompetent persons and incompetent persons without consent from parents, guardians or caregivers. Therefore, if you are aged under 20 years, quasi-incompetent or incompetent, you may proceed to ensure that you have the consent of your parents, guardians or caregivers (in cases where consent is required). If the Companies become aware that the Companies have unintentionally collected personal data of youths without parental consent or collected personal data from quasi-incompetent or incompetent persons without consent from guardians or caregivers, the Companies will delete the aforementioned data immediately or the Companies will collect, use and/or disclose personal data only in the case where the Companies have other law basis beside of the consent.

Thun, if the Companies are unable to collect, use and/or disclose personal data based on the Companies' notifications in this policy, the Companies and affiliates may not be able to perform duties under the employment contract or continue performing duties prescribed by law.

2. Sources of Your Personal Data

The Companies may collect your personal data that you provide directly to the Companies, or the Companies may receive your personal data from other sources.

In cases the Companies collect **your personal data directly from you**, the Companies may receive from the job application process when you submitted to the Companies in accordance with the consideration on recruitment process by registration or full fill on job application forms through the channels specified by the Companies including access to the Companies' website for applying a job and the interviewing process throughout when you start working with the Companies and during in the period of works.

Furthermore, the Companies may **receive your personal data from other sources** as the detail following:

1) Referral, Executive including the affiliated company provided references or recommended you for the Companies.

2) Recruitment agency.

3) Public data sources such as other job application websites, data searched through internet or social media, etc.

4) Government agencies, related agencies, or other persons.

3. Collection, Use and/or Disclosure of Personal Data Under Legal Bases

The Companies collect, use and/or disclose your personal data under other non-consensual legal bases (such as (1) necessity to perform with contracts, enters into a contracts or execute to contracts with you; (2) abiding by Law (3) necessity for lawful benefits of the Companies or other person with balancing for benefits, the rights, and the basic freedom related to your personal data protection (4) for prevention or suspension any perils harmful to life threatening, body or health;(5) the public benefits conducting for the public interest or perform duty in exercising of state power (6) the establishment and fight for the rights to pursuant to the law or other legal base in accordance with personal data protection laws (depending on the case) for the following objectives:

3.1 <u>In cases you are a job applicant, current employee, former employee, contractor, family member or a reference person:</u>

1) **Personnel selection** such as consideration to recruit applicant in position job available of the Companies and affiliates, performing obligation in connection with you regarding the process of selection, interviews, the remuneration as appropriately on the employment procedure. Including to verify the record and other qualifications and/or notification the results of employment selection.

2) **Employment** such as the related processes of hiring and employment contract including other contracts involving the employment such as non-disclosure agreements, policies, and regulations of working, etc.

3) **Employment Relations such as in connecting** with you or related persons to evaluate the work performance, promoting, salary adjustments and special remuneration, personnel capacity improvement, training, work observations, certification of various areas of knowledge and seminars, records of working hours, consideration of vacations, business and sick leave, monitoring your intranet access, email and telephone usage, carry out protocol and steps for resignation, layoffs, compensation payments and/or post-layoff benefits.

4) **Management of finances, remuneration payment and provision of benefits** such payment of remuneration, provision of benefits and privileges for you including management of your health and hygiene such as health insurance, etc., including to disclose your personal data to third parties in term of the benefit related issues such as insurance companies, fund management companies and subcontracting's bank. etc.

5) **Identify proofing** such as verification, proofing and authentical

6) **Protection of the Companies' benefits** such as risk management, audit supervision and internal operation management of the Companies and affiliates, in order to preventing and monitor all operator of fraud, money laundering, criminal actions or any other illegal actions, investigation, interrogation, creation or exercise legal claims, or provision of witnesses and evidence in legal processes of the Companies and affiliates, and for security withing the buildings or other the facilities of the Companies and affiliates including card exchanges before entering the Companies' areas and recording with closed-circuit television cameras (CCTV).

7) **Compliance with the law** such as for the purpose of complying with legal requirements and law enforcement including disclosures or reports to government agencies pursuant to the law such as the Revenue Department and the Anti-money Laundering Office, Department of Skills Development etc., including when the Companies receive directives, court summons or government documents directing the Companies to perform any actions requiring the legal authority of that government agency.

8) **Information technology management** such as information technology management and security.

9) **Prevention or suppression of potential danger to lives, bodies, or health** such as control of communicable diseases or epidemics.

10) **Performing for business operation changes** such as sales, transfers, business mergers, business revitalization or other similar cases in which the Companies may transfer your personal data to one or more third parties as part of the aforementioned actions.

3.2 In cases you are a Shareholder, Director, or Executive of the Companies:

1) **To perform according to the Rights and Duties** such as selection and appointment of directors, contacting to manage or carrying out activities according to authority and duties as Shareholders, Directors, or Executives (such as meetings and consideration of remuneration payments, etc.) and treating you according to the rights and duties as a Shareholder, Director, or an Executive of the Companies.

2) **Proof and identification** such as examination, proof and confirmation of your identity.

3) **Business operations** such as monitoring of your performance, allocation, and management of the Companies' resources to follow-up on responsibilities, monitor discipline, internal audits, and investigations in cases with complaints and/or disciplinary actions (if necessary) to provide support and/or manage relationships with you.

4) **Remuneration payments and privileges** such as payment of dividends, monthly salaries, tax deductions, establishment of provident funds, social security, insurance, compensations including your other privileges.

5) **Protection of the Companies' benefits** such as risk management, audit supervision and internal operation management of the Companies and affiliates which its necessary for creation the exercise legal claims for auditing/confirming the facts to prevent corruption in exercising rights or performing duties pursuant to the law, for verification of identities in the performance of duties according to the positions or authority assigned, risk management, audit supervision, prevention and monitoring all operation of fraud, money laundering, criminal actions or any other illegal actions, investigation, interrogation, creation or exercise legal claims, or provision of witnesses and evidence in legal processes of the Companies and affiliates, and for security withing the buildings or other the facilities of the Companies and affiliates including card exchanges before entering the Companies' areas and recording with closed-circuit television cameras (CCTV).

6) **Compliance with the law** such as for the purpose of complying with legal requirements and law enforcement including disclosures or reports to government agencies pursuant to the law such as the Revenue Department and the Anti-money Laundering Office, the Department of Skill Development etc., including when the Companies receive directives, court summons or government documents directing the Companies to perform any actions requiring the legal authority of that government agency.

7) **Information technology management** such as information technology management and security.

8) **Prevention or suppression of potential danger to lives, bodies, or health** such as control of communicable diseases or epidemics.

9) **Actions in cases where changes occurred in the business** such as sales, transfers, business merging, business recovery or other similar cases in which the Companies may transfer your personal data to one or more third parties as part of the aforementioned actions.

4. Collection, Use and/or Disclosure of Personal Data that Requires Your Consent

The Companies collect, use and/or discloses your personal data under the basis of consent for collection, use and disclosure of sensitive personal data for the following objectives:

1) Health information (such as history of illnesses and medical treatments) for the company's consideration, employment background screening health examinations, leave records, competency

assessments, job assignments and/or appropriately appointment/promotion including health insurance package.

2) Criminal history for employment screening.

3) Biological data for time attendance.

5. Disclosure of Your Personal Data

The affiliates to which the Companies may disclose your personal data, are companies in the Carabao Group, namely, Carabao Group Public Company Limited and subsidiaries, companies in the CJ Group, namely, C.J. Express Group Company Limited and subsidiaries, companies in the TD Group, namely, TD Tawandang Company Limited and subsidiaries, and companies in the Tawandang Group, namely, Tawandang 1999 Company Limited and subsidiaries (**"affiliates"**) for objectives including any actions stated in this policy. Furthermore, affiliates also depend on consent received by the Companies.

If required, the Companies may disclose your personal data to government agencies or any other agencies pursuant to the law such as the Revenue Department, Social Security Office, the Department of Skill Development , Department of Labor Protection and Welfare etc., or disclose data in compliance with any directives from government agencies or regulatory agencies in addition to providing your personal data for credit data agencies in order to check and possibly use the findings from the aforementioned data examination to prevent fraud or corruption.

In some cases, the Companies may be required to disclose or provide your personal data to investors, shareholders, recipients of rights transfers, persons who will receive rights transfers, transferred recipients or persons who will become transferred recipients when the Companies have a corporate restructuring, debt restructuring, business merging, business acquisition, sale, purchase, joint ventures, rights transfers, discontinuation of business or any other similar events and having the Companies' business, assets or shares transferred or distributed whether in whole or in part.

The Companies may disclose your personal data to related third parties such as service providers, business partners, trade partners and contract parties of the Companies to take actions related to audits, legal consultation, prosecution of legal cases, remuneration payment, monthly salary, and any other actions necessary for business operations of the Companies and affiliates. However, the Companies will provide personal data for the other persons only as necessary for the aforementioned services. The Companies will request for the other persons to not use personal data for any other purpose in addition to taking actions to ensure that all other persons with the Companies' work maintain personal data with safety.

The Companies may disclose personal data under legal bases to other persons according to objectives stated in this policy such as ordinary persons, complainers or other persons who requested to see data from closed-circuit television cameras, etc., depending on the case.

6. Transfer of Your Personal Data Abroad

The Companies may disclose or transfer your personal data abroad to other person or servers in destinated countries which may or may not have equivalent personal data protection standards. The Companies will follow steps and measures to ensure personal data is transferred safely and recipient has suitable personal data protection standards and such personal data transfers are legally and permitted by law.

7. Personal Data Storage, Storage Times and Security Measures

The Companies will store your personal data as necessary in line with the objectives stated in this policy. The Companies will consider a suitable time for storing your personal data based on employment contract, tenure, and legal prescription. Furthermore, the Companies may continue to store the aforementioned data as the period necessary for legal compliance, creation and exercise legal claims legal prescription.

The Companies will store personal data in document formats and/or computer or electronic systems by providing appropriate security measures for personal data including administrative safeguards, technical safeguards and physical safeguards in relation to access control for the use of data including appropriate modifications and revisions of measures to prevent loss, illegal access, use, edition, revision or disclosure of personal data without legal authority in order to ensure security of your personal data, confidentiality, integrity and availability.

In particular, the Companies limit access and use technology to maintain safety of your data by requiring permissions or rights to access data with user access management allowing only authorized persons to access data and user responsibilities designation to prevent unauthorized access, disclosure, reveal, smuggling, copies of data or theft of stored data or processing devices. Moreover, the Companies arrange methods to enable retrospective tracing of data accession in relation to access, change, deletion, or transfer. When your data has been disclosed to outside persons that process data or data processors, the Companies will oversee to ensure that such persons have taken appropriate actions in compliance with the Companies' directives.

The Companies will delete or destroy personal data within 30 days from the end of the storage period.

8. Your Rights as the Personal Data Owner

As the data owner, you have the right to withdraw your consent granted to the Companies at any time, except in cases where consent withdrawal is limited by laws or contracts that benefit you. Consent withdrawal does not have effects on processing of personal data which you previously and legally granted to the Companies.

You have the right to request access or copies of personal data collected, used and/or disclosed by the Companies. You have the right to request transfer of your data organized by the Companies in electronically readable format and you have the right to request the Companies to send your personal data to other people

as you intend (the Companies reserve the right to collect appropriate expenses based on real conditions (if any).

You have the right to object the collection, use and/or disclosure of personal data in cases specified by law. You have the right to request the Companies to erase or destroy or make your personal data anonymous by any means as well as the right to suspend use of your personal data except in cases where there are legal limitations.

The Companies will use the best efforts to keep your personal data accurate and up to date for the completion data and not cause misunderstandings. You have the right to request revisions and changes your personal data. When you revise or change your personal data or if you see that data possessed by the Companies is incomplete or inaccurate, this may cause misunderstandings or data may not be up to date. Exercise of your rights specified above must be in compliance with the law and the Companies may refuse your abovementioned rights based on legal limitations.

You have the right to file complaints with authorized officials pursuant to the Act if you are of view that the Companies or other persons working on behalf of the Companies to collect, use and/or disclose your personal data do not comply with the Act. Nevertheless, the Companies would like you to inform the Companies of your concerns to resolve it before contacting the agencies involved.

When submitting a request to exercise your rights, you can contact the Data Protection Officer (DPO) or the person with the duty and responsibility for personal data using contact channels specified in this policy.

9. Cookies

When you visit the Companies' website, the Companies may place cookies in your device and use cookies to collect your personal data. You can study the Companies' cookies policy for more information at https://investor-th.carabaogroup.com/policy.html

10. Policy Changes

The Companies may review and revise this policy to be consistent with any changed rules and regulations. If the Companies modified, changed or made revisions to this policy, the Companies will publicize the revision through appropriate channels such as notifications on the Companies' website, etc. Please check this policy periodically to see revisions or modifications made. The Companies will remind you if the revision have significantly affected you, the company will request your re-consent on the necessity and when legally required to do so.

11. Contact Channels

You can contact the Companies and/or Data Protection Officers (DPOs) via the following channels in cases where you have additional recommendations or questions concerning protection for your personal data:

Carabao Group Public Company Limited and Subsidiaries

- Place of Contact: Carabao Group Public Company Limited
  393, 393 Silom Building 7th - 10th floor, Silom Road, Silom, Bangrak, Bangkok, 10500
- Contact Channels: Tel. 02-636-6111

For a Data Protection Officer (DPO) or a person the duties and responsibilities for your personal data, you can contact Email: PDPA@carabao.co.th.