BAKER TECHNOLOGY LIMITED & SUBSIDIARIES

(collectively "Group")

CORPORATE OPERATING PROCEDURES

Personal Data Protection Policy

Revision	Date	Remarks	Document and Revision number	Prepared	Approved
1	6 Aug 19	Approved for Use	BTL-SOP-CORP-005	JC	Board
2	15 May 23	Approved for Use	BTL-SOP-CORP-005	JC	Board

This is a Controlled Document
All queries, suggestions, interpretation, clarification or change request shall be addressed at the first instance to the CEO or if unavailable his delegate.

Table of Contents

INTRODUCTION

Baker Technology Limited and its group companies ("Group", "us", "we") is committed to protecting your Personal Data. We aim to treat your Personal Data with the highest level of confidentiality and care.

This Personal Data Protection Policy ("Policy") applies to all departments, business units and companies/subsidiaries within the Baker Technology Group and sets out the principles and procedures that Baker Technology Group has in place to comply with the requirements of the Personal Data Protection Act 2012 ("PDPA"). Each subsidiary / company within the Group will implement and maintain appropriate safeguards of Personal Data including Personal Data which is shared among the Group.

The online shortened version of the Policy is available on our Group company websites while this detailed Policy will be made readily available to employees together with our employee handbook.

POLICY STATEMENT

During the course of the Group's activities, we may collect, store and process personal information about employees, customers, suppliers, vendors, clients, shareholders and other stakeholders and we recognise the need to treat this data in an appropriate and lawful manner. We are committed to complying with our obligations in this regard in respect of all Personal Data we handle. We only collect Personal Data that is relevant to our business and/or employment relationship with you.

The types of information that the Group may be required to handle include details of current, past and prospective employees, suppliers, customers, and others that the Group communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Personal Data Protection Act 2012 and other regulations ('the Acts'). The Acts impose restrictions on how we may collect and process that data.

This Policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this Policy will be taken seriously and may result in disciplinary action up to and including dismissal on any of our employees.

PURPOSE AND SCOPE OF THE POLICY

This Policy sets out the Group's rules and guidelines on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal information.

The Policy applies to all departments, business units and subsidiaries within the Baker Technology Group as well as individual employees and board members of the Group and any third party service provider who agrees to abide by this Policy by way of contract

If an employee considers that the Policy has not been followed in respect of Personal Data about themselves or others they should raise the matter with their manager as soon as possible.

DEFINITION OF DATA PROTECTION TERMS

"Personal Data" means data relating to a living individual who can be identified from that data (or from that data and other information that is in, or is likely to come into, the possession of the Company). Personal

Data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Personal Data can be in the form of any electronic or hard copies.

However Personal Data does not include

- business contact information
- personal data in relation to a deceased individual who has been dead for more than 10 years
- publicly available information which cannot be associated with an individual or which has been anonymised

"Data Users" include employees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following the Group's Policy at all times.

The Data Users within the Group include:

- HR/Admin department
- Finance department
- QAQC department
- HSE department
- Security department
- Senior Management

"Data Intermediaries" are individuals or organisations which may be contracted to use or process Personal Data on behalf of the Group for example our insurance broker.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data.

DATA PROTECTION PRINCIPLES

Anyone processing Personal Data must adhere to the following obligations, namely:

- the Consent Obligation
- the Purpose Limitation Obligation
- the Notification Obligation
- the Access and Correction Obligation
- the Accuracy Obligation
- the Protection Obligation
- the Retention Limitation Obligation
- the Transfer Limitation Obligation
- the Openness Obligation

CONSENT OBLIGATION

The Consent Obligation prohibits organisations from collecting, using or disclosing an individual's Personal Data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. Exceptions to obtaining consent can occur only if such exception is authorised under the PDPA or any other written law.

The nature and type of data the Group collects and the source of such data varies depending on the nature of the relationship the Group has with the data subject.

Personal Data is used to manage employment relationships, safety and security reasons, support of subcontractor manpower, manage shareholder lists among other reasons including:

- consideration of job application for employee recruitment
- performance appraisal
- to meet regulatory and legal requirements
- for risk management (security and safety)
- payment of salary and CPF
- application of work visa
- for all other purposes incidental and associated with the above.

The Personal Data Inventory (Appendix 1) indicates the types of Personal Data collected, who, how & why the data is collected and when consent is obtained and the Data Subject is notified of the purpose, who the Data Users are and to whom the personal data is disclosed to. The Personal Data Inventory will be reviewed and updated as required every 6 months.

Consent from an individual is only considered to have been provided if such individual has been notified of the purposes for which his personal Data will be collected, used or disclosed and such individual has provided his/her consent for those purposes. Consent can be provided in writing/recording or verbally (although this is less preferred). Consent can also be implied or inferred:

- Deemed consent by conduct: from the circumstances or conduct of the individual eg actively providing the information or continuing to attend a conference even though the event is recorded
- Deemed consent by contractual necessity: where disclosure to other parties is required for a contract to be fulfilled eg
- Deemed consent by notification: Where the individual has been notified of the purpose and has not opted out of the collection, use or disclosure of his Personal Data. The Group should mitigate any adverse effects of the disclosure

Third parties from whom the Group collects Personal Data from should be able to provide consent for the collection, use and disclosure of Personal Data on behalf of the individual or demonstrate that the third-party source had obtained consent for the disclosure of the Personal Data. Examples of such third parties would be subcontractors for whom the Group supports the application and issue of work permits for some foreign workers.

The Group also relies on the legitimate interests exception to collect, use or disclose Personal Data for purposes of security, prevention and detection of fraud, misuse of services and to manage to disputes among others.

The Group is aware that individuals have the right to withdraw their consent to the collection, use or disclosure of their Personal Data for any purpose.

Individuals who would like to submit a notice to withdraw their consent for specific purposes should submit their notice by sending an email to the Group Personal Data Protection Officer ("PDPO"). The contact details are in Clause 0. The individual should provide a minimum of 30 days' notice to withdraw his consent.

The Group is aware that certain services it provides and the continuation thereof may require the collection, use and disclosure of such data. Failure to collect, use and disclose such data may result in discontinuation of such services including potentially termination of employment or business relationships.

Upon receiving the withdrawal notice, the PDPO shall inform the individual of the likely consequences of withdrawing his consent. If the individual still wishes to proceed with the withdrawal of consent, the Group shall cease the collection, use and disclosure of the Personal Data within 30 days. The Group shall ensure that consent withdrawal requests and outcomes are properly documented and acted upon in a timely manner.

In addition, the Group will also inform all data intermediaries about the withdrawal of consent and ensure that they cease collecting, using or disclosing the Personal Data.

The withdrawal of consent for the collection, use or disclosure of Personal Data does not require the Group to delete or destroy the individual's Personal Data. The Personal Data can still be retained in accordance with the Retention Limitation Obligation.

If ad-hoc requests for the disclosure of Personal Data are made to the Company which are not covered by the scenarios as per the Data Inventory Map, specific consent should be sought from the individual in writing prior to the disclosure of the Personal Data.

Examples of such requests include:

- Bank reference checks (when employees apply for bank loans)
- Employment reference (when employees apply for positions in other companies)

PURPOSE LIMITATION OBLIGATION

The Group may only collect, use or disclose Personal Data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and for which the individual was notified.

The Group should not collect, use or disclose Personal Data when the purposes for which the Personal Data were collected is no longer valid and should not collect excess personal data than what is required for the specific purposes.

Should Personal Data be required for new purposes, fresh consent should be obtained.

NOTIFICATION OBLIGATION

When collecting Personal Data from an individual, the individual must be informed of the purposes for which and how such Personal Data will be used.

The Group has included a statement of purposes in HR forms and letters (including job application forms, post hire forms, employment agreements) used for collecting Personal Data as well as at other points of data collection including at our security guard house.

In order to obtain consent for the collection, use and disclosure of Personal Data, the individual must be informed of

- The purposes of collecting the data and
- Upon request, the contact details of the PDPO whom they can contact regarding the collection, use and disclosure of Personal Data

However, the Notification Obligation does not apply when the individual is deemed to have given consent (as per the PDPA) or the Group is collecting, using or disclosing Personal Data without the consent of the individual in accordance to the circumstances specified in the PDPA (for example for performance evaluation purposes)

Links to the Group's Personal Data Protection Policy (online version) are also provided to individuals at the point of collection. Employees are also given the Group's Personal Data Protection Policy (internal version).

ACCESS AND CORRECTION OBLIGATION

The Group must, upon request, (i) provide an individual with his or her Personal Data in the possession or under the control of the Group and information about the ways in which the Personal Data may have been used or disclosed during the past year subject to any relevant exception in the PDPA; and (ii) correct an error omission in an individual's Personal Data that is in the possession of under the control of the Group.

Any individual requesting access to Personal Data may submit their request to the PDPO.

The Group is only required to provide Personal Data that the individual has requested for and is entitled to have access to under the PDPA and only if it is feasible for the Group to do so. Information which is no longer within the Group's possession or under its control upon receiving the access requested will not be provided.

If the individual making the access request asks for a copy of his Personal Data in documentary form, the Group will charge a fee for producing the copy. If such Personal Data cannot be practicably provided to the individual in documentary form (e.g. CCTV footage which cannot be extracted), then the Group may provide the individual with a reasonable opportunity to examine the requested data in person.

Access requests will only be granted if the burden or expense of providing access is not unreasonable, frivolous or vexatious.

An individual may submit a request to correct an error or omission in the individual's Personal Data that is in the possession or under the control of the Group to the PDPO.

Upon receipt of a correction request, the Group is required to consider whether the correction should be made. If the correction should be made, the PDPO should ensure that the Personal Data is corrected as soon as practicable and send the corrected Personal Data to every other company to which the Personal Data was disclosed by the Group within a year before the correction request was made, unless that other company does not require the corrected Personal Data for any legal or business purpose.

The PDPA provides exceptions under which the Group is not required to correct Personal Data despite receiving such a correction request.

All access and correction requests will be responded to within 30 days:

- For access requests, the PDPO will reply to the individual with a written estimate of the fee to fulfil the access request, the requested information or the time by which the Group will be able to respond to the request.
- For correction requests, the PDPO will ensure that the data is corrected within the time frame or inform the individual of the time by which the Group will be able to respond to the request.

ACCURACY OBLIGATION

This obligation is to ensure that where Personal Data may be used to make a decision that affects the individual, that the Personal Data is accurate and complete, however the Company is not required to check the accuracy and completeness of the individual's personal data each and every time it makes a decision about the individual.

Personal Data provided by an individual will be assumed to be accurate however where the currency (when the Personal Data was obtained) of the Personal Data is important, the Group will take steps to verify that the Personal Data is up to date before making a decision that will significantly impact the individual.

Third parties who provide Personal Data to the Group will be asked to verify the accuracy and completeness of that Personal Data.

PROTECTION OBLIGATION

The Group is required to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

The following are some of the measures that the Group has in place:

- Employees are bound by confidentiality obligations in their employment agreements.
- The Group ensures that only the appropriate amount of personal data is held.
- Confidential documents are stored in locked file cabinets.
- Access to confidential documents is restricted to employees on a need to know basis
- Confidential documents that are no longer required are properly disposed
- Ensure that computer networks are secure through password protection and firewalls

- Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period
- Installing appropriate computer security software and using suitable computer security settings
- Ensuring that IT service providers are able to provide the requisite standard of IT security
- Visitors arriving at security are signed in by security and so visitors are unable to obtain access to other visitors' Personal Data
- Senior management offices are locked to prevent unauthorised access

RETENTION LIMITATION OBLIGATION

The Group is required to cease to retain documents containing personal data or anonymise the data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by the retention of the personal data and the retention is no longer necessary for legal, tax and business purposes.

For legal, tax and business purposes, the Group retains Personal Data for 7 years except in specific circumstances for example:

- The employee is still employed by the Group in which case copies of the data may be retained until 7 years after employment ceases
- A subcontractor worker's work permit is still being supported by the Group in which case copies of the data may be retained until 7 years after the support ceases

Upon determination that the Personal Data is no longer required, the Group will make reasonable efforts to cease to retain the Personal Data by:

- Returning the documents to the individual or
- Destroying the documents by shredding or disposing of them in an appropriate manner or
- Anonymising the Personal Data or
- Deleting soft copies from the server to the extent possible without requiring formatting of the server

TRANSFER OBLIGATION

The Group is restricted from transferring any Personal Data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that the Group provides a standard of protection to Personal Data so transferred that is comparable to the protection under the PDPA.

The Group will take appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations to provide to the Personal Data transferred a standard of protection that is comparable to that under the PDPA.

OPENNESS OBLIGATION

The Group has appointed a Personal Data Protection Officer whose responsibilities are as follows:

Review data protection and related policies and procedures, advising other employees on data protection issues and providing training as required

- Act as a contact point for internal and external PDPA related queries (contact details made available publicly) and liaise with the Personal Data Protection Commission when necessary
- Identify cases that breach the PDPA and initiate remedial actions including investigating the breach, identifying the timeframe and also the Personal Data Protection Commission (if necessary)
- Review contracts with third parties to ensure data protection provisions are covered when required
- Raise awareness about data protection within the Group and advise departments on the PDPA when appropriate
- Acknowledge, evaluate and oversee access/correction/consent withdrawal requests.
- Address any inquiries by individuals, authorities and employees regarding data protection and information received from individuals and from the authorities
- Address queries about the Group's reliance on the legitimate interests exception
- Monitor implementation of data protection standards, policies and procedures within the Group
- Monitor, review and update the Personal Data Inventory on a regular basis
- Maintain a record of third parties service providers to which the Group discloses or transfers Personal Data. See Appendix 2

The appointed PDPO is Jeanette Chang, CEO

The contact details of the PDPO are as follows:

pdpo@bakertech.com.sg
Personal Data Protection Officer
Tel: 6262 1380
10 Jalan Samulun
Singapore 629124

EMPLOYEE TRAINING

Employees who will have access to any kind of Personal Data will have their responsibilities especially with respect to the Policy outlined on their first day. All employees will also be provided with the Policy in the employee handbook.

BREACH OF PDPA AND COMPLAINTS

In the event of a breach of or loss of Personal Data, the Group must respond to and manage the incident promptly and effectively. Any issues relating to Personal Data Protection shall be escalated to the PDPO for review, followed by investigation and / or escalation to the Management team if necessary. The course of action follows four key steps (using the acronym C.A.R.E)

Steps that might be taken to Contain the breach:

Conduct an initial appraisal of the breach

- Identify the root cause of the breach
- Number of affected individuals
- Type(s) of personal data involved

  - Affected systems, servers, databases, platforms, services etc
  - Whether help is required to contain the breach
  - Remedial action(s) to reduce harm to affected individuals
- **Shut down the compromised system that led to the data breach**
  - Isolate compromised system from the internet or network
  - Re-route / filter network traffic, firewall filtering, closing particular ports / mail servers
  - Prevent further unauthorised access to the system. Disable / reset passwords
  - Isolate causes of data breach and where applicable, change access rights to compromised system
- **Establish whether lost data can be recovered and implement further action to minimise any damage caused by the breach**
- **Put a stop to practices that led to the data breach including improving on protection procedures and retraining involved employees**
- **Notify the authorities (eg Police or Cyber Security Agency of Singapore) if criminal activity is suspected**

Steps that might be taken to **Assess** the breach, success of containment action(s) taken or the efficacy of any technological protection applied on the Personal Data.

An assessment should be conducted to assess whether the data breach is notifiable under the PDPA and the steps taken to assess the data breach should be documented. The assessment should not take longer than 30 days.

The following should be considered when assessing the data breach:

- **Context of the data breach**
  - Types of Personal Data involved
  - Individuals whose Personal Data have been compromised (eg minor, vulnerable individuals etc)
  - Other contextual factors eg whether the Personal Data was publicly available before the data breach
- **Ease of identifying individuals from the compromised data**
  - Depends on the number and uniqueness of identifiers in the compromised data. There should at least be two data elements for an individual to be identified.
- **Circumstances of data breach**
  - Was the Personal Data illegally accessed and stolen vs accidentally sent to recipients
  - How long has the compromised data been made publicly accessible before the data breach was discovered
- **Determine the risk and impact to the Group:**
  - What caused the data breach
  - When did the breach occur and did it occur more than once
  - Who might gain access to the compromised Personal Data
  - Will the compromised data affect transactions with any other third parties

Reporting the breach

The Personal Data Protection Committee ("PDPC") must be notified of breaches that

- **result in, or is likely to result in, significant harm to the affected individuals; or**
- **are of a significant scale (involves Personal Data of 500 or more individuals).**

The PDPC has to be notified as soon as is practicable but in any case no later than 3 calendar days after the day the Group has made the assessment that a data breach is a notifiable data breach.

Affected individuals must also be notified if the data breach is likely to result in significant harm to them. Personal Data which are deemed to result in significant harm to affected individuals include authentication data relating to an individual's account with an organisation, credit card information, bank account number, creditworthiness of an individual, salary information etc). Affected individuals should be notified as soon as practicable, at the same time or after notifying the PDPC.

The notification is to include the following information:

- **Date on which and circumstances in which the Group first became aware that the data breach had occurred**
- **Chronological account of steps taken by the Group after becoming aware of the breach including the Group's assessment that the data breach is notifiable**
- **Information on how the notifiable data breach occurred**
- **Number of affected individuals**
- **Personal Data or classes of Personal Data affected**
- **Potential harm to the affected individuals**
- **Information on any action by the Group to:**
    - Eliminate or mitigate any potential harm to any affected individual; and
    - Address or remedy any failure or shortcoming that the Group believes to have caused, or enabled or facilitated the occurrence the notifiable data breach
- **Information on the Group's plan (if any) to inform all or any affected individual / public that the notifiable breach had occurred and how an affected individual may eliminate or mitigate any potential harm**
- **Business contact information of at least one authorised representative of the Group**

Evaluate the response and recovery to prevent future breaches. Depending on the specific situation, the evaluation process could involve:

- **A review including a root cause analysis of the data breach (eg implement fixes to system errors / bugs to prevent future disclosure of/access to personal data)**
- **A prevention plan to prevent similar data breaches in the future**
- **Audits to ensure that the prevention plan is implemented**
- **A review of existing policies, procedures and changes to reflect the lessons learnt from the review**
- **Changes to employee selection and training practices**
- **A review of data intermediaries involved in the data breach**
- **Consider the following issues:**
    - Operational and policy related issues
    - Resource related issues
    - Employee related issues
    - Management related issues

Continuing efforts should also be made to prevent further harm from the data breach.

All complaints in relation to this Policy or any PDPA related matters can be made to the PDPO. The PDPO will respond to the complaint within 30 days.

PENALTIES FOR BREACH OF PDPA

For breach of the PDPA, the PDPC can impose financial penalties on the Group. Such penalties would be the higher of:

- **Up to 10% of annual turnover in Singapore; or**
- **S$1 million**

Individuals will also be held accountable for egregious mishandling of Personal Data including the following criminal offences:

- **Knowing or reckless unauthorised disclosure of Personal Data;**
- **Knowing or reckless unauthorised use of Personal Data for a wrongful gain or wrongful loss to any person; and**
- **Knowing or reckless unauthorised reidentification of anonymised data.**

The penalty for such criminal offences will be a fine not exceeding S$5,000 or imprisonment for a term not exceeding 2 years or both.

DATA PORTABILITY

Individuals will have the right to data portability and therefore at the request of the individual, organisations must transmit an individual personal data that is in the organisation's possession or under its control, to another organisation in a common machine readable format.

APPENDIX

Appendix 1 Inventory Map

Revision History

Rev No.	Issue Date	Description of Changes	Clause #	Signature
0	31/8/16	Initial release	N.A.	
1	6/8/19	Revised Formatting		
2	15/5/23	Update to meet PDPA 2012 revisions	Multiple	