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

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

1. INTRODUCTION

1.1 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.

1.2 This Personal Data Protection Policy ("Policy") applies to all departments, business units and 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").

1.3 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

2. POLICY STATEMENT

2.1 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.

2.2 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.

2.3 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.

3. PURPOSE AND SCOPE OF THE POLICY

3.1 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.

3.2 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

3.3 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.

4. DEFINITION OF DATA PROTECTION TERMS

4.1 "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

4.2 "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
- HSE department
- Security department
- Senior Management

4.3 "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.

4.4 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.

5. DATA PROTECTION PRINCIPLES

5.1 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

6. CONSENT OBLIGATION

6.1 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.

6.2 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.

6.3 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 and 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.

6.4 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.

6.5 The Group is aware that individuals have the right to make a choice not to provide their Personal Data and may revoke their consent to the collection and processing of personal data.

6.6 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 14.3. The individual should provide a minimum of 30 days' notice to withdraw his consent.

6.7 The Group is aware that certain services it provides and the continuation thereof may require the processing of such data. Failure to process such data may result in discontinuation of such services including potentially termination of employment or business relationships.

6.8 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.

6.9 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.

6.10 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.

6.11 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)

7. PURPOSE LIMITATION OBLIGATION

7.1 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.

7.2 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.

7.3 Should Personal Data be required for a new purpose, fresh consent should be obtained.

8. NOTIFICATION OBLIGATION

8.1 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.

8.2 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.

8.3 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

8.4 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)

8.5 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).

9. ACCESS AND CORRECTION OBLIGATION

9.1 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.

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

9.3 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

9.4 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.

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

9.6 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.

9.7 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.

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

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

- 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

10. ACCURACY OBLIGATION

10.1 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.

10.2 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.

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

11. PROTECTION OBLIGATION

11.1 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.

11.2 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

12. RETENTION LIMITATION OBLIGATION

12.1 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.

12.2 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

12.3 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

13. TRANSFER OBLIGATION

13.1 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.

13.2 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.

14. OPENNESS OBLIGATION

14.1 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
- 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

14.2 The appointed PDPO is Jeanette Chang, CEO

14.3 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

15. EMPLOYEE TRAINING

15.1 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.

16. BREACH OF PDPA AND COMPLAINTS

16.1 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.

16.2 Steps that might be taken to contain the breach:

- Identify the root cause of the breach
- Shut down the compromised system that led to the data breach
- Establish whether steps can be taken to recover lost data and limit 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
- Carry out an IT check if the breach is related to the IT network. Change passwords, access rights and temporarily interrupt external connections to the system
- Notify the authorities if criminal activity is suspected

16.3 Steps that might be taken to assess the risks and impact

- Determine the risk and impact to individuals:
  - Number of people affect
  - What group of people's Personal Data had been breached
  - What types of Personal Data was involved
  - What additional measures were in place to minimise the impact of a data breach

- 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

16.4 Evaluate the response and recovery to prevent future breaches. Consider the following issues and what can be done to prevent a repeat of the data breach:

- Operational and policy related issues
- Resource related issues
- Employee related issues
- Management related issues

16.5 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.

17. **APPENDIX**

Appendix 1 Inventory Map

What is collected?	Why is it collected?	Who collects it?	How is it collected?	Is Consent obtained / is Notification provided?	Where is it stored?	Who is it disclosed to?
Candidates / Employees						
- Personal particulars e.g. name, ID number, passport number, mobile number, email address, address, date of birth, - Personal academic details - Previous experience - Existing medical conditions - Existing financial health	- For job interiew purposes so that we can evaluate the person for job suitability - contact details are collected for ease of communication if we want to make an offer or call back for another interview	- HR/admin personnel & Exec Director collect the information - Department manager if the candidate is referred to them	- Candidate submits the details to us directly - We ask the candidate to fill in an Application Form - job agencies send us the details	- Candidates consents within the Application Form and is also notified about the use of personal data	- If the information is emailed to us, then it is stored in our email server and also in soft copy on our hard drives - hard copies are also provided to the interviewers (Exec Director and Head of Department)	- HR / admin personnel, Exec Director and Head of Department
Additional particulars: - employment start and end dates - salary details - bank details	- Upon hiring, the data is used for managing the employment relationship - paying salary and CPF - submission to IRAS for individial tax purposes - inclusion in the company health benefits programme (insurance) - applying for work permit, S Pass or EP if required - signing up for training programmes	- HR/admin personnel & Exec Director collect the information	- Post Hire Form is provided to the employee - Signed employment agreement	- Employees consent within the Post Hire Form and are also notified about the use of personal data (for managing employment relationship)	- soft copies on email server and hard drive (HR/admin, Finance) - hard copy in personal folders (HR/Admin)	- HR / admin personnel & Exec Director - Senior Finance department personnel (Name, ID, Address, employment details, bank details, Employment agreement) - our bank for interbank transfers for payments - regulatory bodies for the payment of CPF and also submission of individual statements to IRAS and for other claims eg NS, childcare, paternity, maternity - Insurance broker and insurer (employee benefits and WIC) (name, ID numbers, employment details) - MOM for application of work visas
Emergency contact details:	- to ensure that we have an alternative contact if we have to contact the employee urgently and is not able to or to inform the emergency contact if there is an emergency involving the employee	- HR/admin personnel collect the information	- Post hire form is provided to the employee	- Employees consent within the Post Hire Form and are also notified about the use of personal data (for managing employment relationship)	- soft copies on hard drive (HR/admin, Finance) - hard copy in personal folders (HR/Admin)	- HR / admin personnel & Exec Director
Medical details (invoices, medical reports)	- for insurance claims - for claims for medical costs and medical leave - for submission to MOM if required	- HR/admin personnel & Exec Director collect the information - Employee's supervisor	- invoices and records are provided by the employee to the Company - Hospital/clinic sends the documents directly to the Company or to our Insurer	- Employees consent through the employment agreement	- Softcopy on email and hard drive - Hard copy in Insurance claim folder kept with HR - hard & soft copy of invoices kept with Finance	- HR / admin personnel & Exec Director - Finance who processes the claims (only invoices) - Insurance broker - Insurer - HSE if there is a work related injury - MOM if there is a work related injury
Academic and training certificates	- to demonstrate that the candidate / employee has the training and certification to take on certain roles eg forklist driver, rigger or qualifies acadamically for their position (e.g degree cert)	- HR/admin personnel & Exec Director collect the information - QA/QC if testing and certification is carried out by QA/QC	- Employee provides us with the certificates (usually at interview or hiring stage) - Training centre provides us with the certificates if we sponsor the training	- Candidates consents within the Application Form (though not explicitly in relation to certificates) and is also notified about the use of personal data - No consent required for trainings that we sponsor	- Soft copy on email and hard drive - Hard copy in Training folder - Hard copy in Personal Folder - Hard and soft copy with HSE (safety related certificate)	- HR / admin personnel & Exec Director - HSE personnel - Training centres (in addition to name and IC number for booking purposes) - WDA and other regulatory bodies for grant submission
Company communications to employees eg. Loan letters, changes in salary, bonus letters, cash advance	- Company communication is issued by the Company and is kept as a record of changes in the employment agreement	- HR/admin personnel and Exec Director	- the letter is issued by HR/Admin personel or Exec Director	- no	- soft copies on email or hard drive - hard copies in their personal folder	- HR/admin personnel - Finance (finance related letters)
Photograph	- to provide C and G cards for access on site - Annual report photos	- HR/admin personnel - IR personnel or 3rd party photographer	- a photo of the employee is taken in the office	- We verbally inform the employee that we are taking their photo for the C&G card or promotional material - we verbally inform the employee of the purpose	- Soft copy on email & hard drive - on the C&G card that we produce inhouse - in the published annual report	- HE/admin personnel - IR personnel - 3rd party designer of our annual report - Printer of annual report
Thumbprint	- To time management / clock in and out purposes	- HR/admin personnel	- the thumbprint is directly recorded into the thumbprint scanner	- We verbally inform the employee of the purpose of collection	- in soft copy on the machine	- The thumbprint data is not accessed by anyone as there is no need to
Dependents' personal details	- to aid our employee to apply for Dependent Pass	- HR/admin personnel	- The employee provides the data to the HR/Admin personnel verbally or via email	- the information is willingly provided by the employee and the employee is aware that such information is to be used for Dependent Pass application - the employee acknowledges in a letter that the information is provided by him	- in soft copy in email server and hard drive - in hard copy in Personal Folder	- HR/admin personnel - Finance (only letter signed by employee, naming the dependent and agreeing to pay the issuance fee) - MOM

Personal details as required for travel bookings and visa applications	- collected as per above - to book work related travel	- collected as per above	- collected as per above	- consent for collection is obtained in the Application Form - notification for travel purposes is not explicitly obtained except under "manage employment relationship"	- stored as above	- in addition to those named above: travel agent or online booking, agency for visa application, embassy/high com
Personal details as required for picking up of documentation (specific to drivers)	- collected as per above - to enable the driver to pick up documents etc with the necessary authorisation letter (usualy including their name and IC number)	- collected as per above	- collected as per above	- consent for collection is obtained in the Application Form - specific consent for this purpose is not obtained but the driver is aware that we have provided his details in an authorisation letter (he carries that with him)	- stored as above	- in addition to those named above: Whomever the driver is picking up an item for (only when an authorisation letter is required)
CCTV	- for safety and security reasons	- captured by CCTV	- captured by CCTV	- a sign is displayed at the entrance of the yard notifying all visitors and staff that there is CCTV	- in soft copy in the CCTV server	- Senior management - Security - HSE - Regulators if requested
Subcontractors						
Personal data (as per IC, FIN or driving licence)	- for safety and security reasons to access/work in our yards - for HSE records - for submission to MOM to support work permits	- Security - HSE - HR/Admin	- Provided by subcontractor company/supervisor - provided to security - provided to HR/Admin for support of workers (WP)	- Consent should be obtained by the subcontractor company - our responsibility is only for Retension and Protection	- hard copy with security - hard and soft copy in email and hard drive	- Security - HSE - HR/Admin - MOM
Other personal data (passport details, marriage status, nationality, salary etc)	- for submission to MOM to support work permits	- HR/Admin	- Provided by subcontractor company	- Consent should be obtained by the subcontractor company - our responsibility is only for Retension and Protection	- hard and soft copy in email and hard drive	- HR/Admin - MOM
Visitors						
Personal data (as per IC, FIN or driving licence), mobile number and vehicle plate number	- for safety and security reasons - also for carpark lot issuance purposes	- Security	- Visitors have to provide their IC, FIN/WP card, Driving licence to security who will record the information - the visitor will also provide their mobile number	- visitors provide consent by providing the information to security - a sign will be installed to notify visitors of the need for the information	- in hard copy in the guard house	- Security
Shareholders						
Personal data including shareholding in Baker Tech shares	- for us to manage our share register	- CDP - Share registrar	- electronic through standard share holding mechanisms	- consent is deemed to have been provided as the information is provided by the shareholder to the share registrar	- soft copy in email server and hard driver - hard copy	- Exec Directors and Tan YG '- Company Secretary '- Share registrar

Appendix 2 List of Third Party Access

Group Companies with access to Personal Data of other Group Companies

Personal Data of Company A	Company B which has access to such Personal Data	Data User in Company B
Baker Engineering Pte. Ltd.	Baker Technology Limited	Executive Director (all data) CFO (salary related data) Board of Directors (bonus related data)
Sea Deep Shipyard	Baker Technology Limited	Executive Director (all data) CFO (salary related data) Board of Directors (bonus related data)
	Baker Engineering Pte. Ltd.	HR Executive (attendance data, medical data, some HR personal data) Exec Director Secretary (medical data, some HR personal data)
Interseas Shipping	Baker Technology Limited	Executive Director (all data) CFO (salary related data) Board of Directors (bonus related data)
	Baker Engineering Pte. Ltd.	HR Executive (attendance data, medical data, some HR personal data) Exec Director Secretary (medical data, some HR personal data)
BT Investment	Baker Technology Limited	Executive Director (all data) CFO (salary related data) Board of Directors (bonus related data)

List of Data Intermediaries:

- Jardine Lloyd Thompson: Insurance brokers
- Mercers: Previous employee benefits insurance brokers (contract ended in early 2014)

List of Third Parties:

- Regulatory bodies
- Training centres
- Aviva Ltd
- ACE Limited
- Foreign Worker Dormitories

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		