DATA PROTECTION POLICY

Palo IT SG respects the privacy of its employees and shall collect and handle personal data of employees in compliance with the requirements of the Personal Data Protection Act 2012 of Singapore and its regulation(s) ("PDPA").

This Data Protection Policy ("Policy") sets out the basis upon which the Company ("we", "us" or "our") may collect, use, disclose or otherwise process personal data of employees and job applicants in accordance with the PDPA. This Policy applies to personal data in our possession or under our control, including personal data in the possession of organizations that we have engaged to collect, use, disclose or process personal data for our purposes.

1. APPLICATION OF THIS POLICY

This Policy applies to all persons engaged in a contract of service with us (whether on a part-time, temporary or full-time basis) and interns and trainees working at or attached to us (collectively referred to as "employees") as well as persons who have applied for any such position with us ("job applicants"), and all references to "employment" shall apply equally to internships and traineeships (as may be applicable).

2. PERSONAL DATA

2.1. As used in this Policy, "personal data" means data, whether true or not, about an employee or a job applicant who can be identified: (a) from that data; or (b) from that data and other information to which we have or are likely to have access.

2.2. If you are a job applicant, personal data which we may collect includes, without limitation, your: (a) name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth; (b) mailing address, telephone numbers, email address and other contact details; (c) resume, educational qualifications, professional qualifications and certifications and employment references; (d) employment and training history; (e) work-related health issues and disabilities; and (f) photographs.

2.3. If you are an employee, personal data which we may collect in the context of your employment with us includes, without limitation, your: (a) name or alias, gender, NRIC/FIN or passport number, date of birth, nationality, and country and city of birth; (b) mailing address, telephone numbers, email address and other contact details; (c) employment and training history; (d) salary information and bank account details; (e) details of your next-of-kin, spouse and other family members; (f) work-related health issues and disabilities; (g) records on leave of absence from work; (h) photographs and other audio-visual information; (i) performance assessments and disciplinary records; and (j) any additional information provided to us by you as a job applicant (that is, prior to being engaged as an employee).

2.4. Other terms used in this Policy shall have the meanings given to them in the PDPA (where the context so permits).

3. COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

3.1. We generally collect personal data that (a) you knowingly and voluntarily provide in the course of or in connection with your employment or job application with us, or via a third party who has been duly authorized by you to disclose your personal data to us (your "authorized representative", which may include your job placement agent), after (i) you (or your authorized representative) have been notified of the purposes for which the data is collected, and (ii) you (or your authorized representative) have provided written consent to the collection and usage of your personal data for those purposes, or (b) collection and use of personal data without consent is permitted or required by the PDPA or other laws.

We shall seek your consent before collecting any additional personal data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorized by law).

3.2. If you are a job applicant, your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes: (a) assessing and evaluating your suitability for employment in any current or prospective position within the Company, and (b) verifying your identity and the accuracy of your personal details and other information provided.

3.3. If you are an employee, your personal data will be collected and used by us for the following purposes and we may disclose your personal data to third parties where necessary for the following purposes:

(a) performing obligations under or in connection with your contract of employment with us, including payment of remuneration and tax;
(b) all administrative and human resources related matters within the Company, including administering payroll, granting access to our premises and computer systems, processing leave applications, administering your insurance and other benefits, processing your claims and expenses, investigating any acts or defaults (or suspected acts or defaults) and developing human resource policies;
(c) assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position within the Company;
(d) ensuring business continuity for the Company in the event that your employment with us is or will be terminated;
(e) performing obligations under or in connection with the provision of our goods or services to our clients;
(f) facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of the Company, or corporate restructuring process; and
(g) facilitating our compliance with any laws, customs and regulations which may be applicable to us.

4. WITHDRAWING CONSENT BY JOB APPLICANTS

4.1. The consent that you provide for the collection, use and disclosure of your personal data will remain valid until such time it is being withdrawn by you in writing. If you are a job applicant, you may withdraw consent and request us to stop using and/or disclosing your personal data for any or all of the purposes listed above by submitting your request in writing or via email to our Data Protection Officer at the contact details provided below.

4.2. Upon receipt of your written request to withdraw your consent, we may require reasonable time (depending on the complexity of the request and its impact on our relationship with you) for your request to be processed and for us to notify you of the consequences of us acceding to the same, including any legal consequences which may affect your rights and liabilities to us. In general, we shall seek to process and effect your request within 30 days of receiving it.

4.3. Whilst we respect your decision to withdraw your consent, please note that depending on the nature and extent of your request, we may not be in a position to process your job application (as the case may be). We shall, in such circumstances, notify you before completing the processing of your request (as outlined above). Should you decide to cancel your withdrawal of consent, please inform us in writing in the manner described in paragraph 30.1 above.

5. ACCESS TO AND CORRECTION OF PERSONAL DATA

5.1. If you wish to make (a) an access request for access to a copy of the personal data which we hold about you or information about the ways in which we use or disclose your personal data, or (b) a correction request to correct or update any of your personal data which we hold, you may submit your request in writing or via email to our Data Protection Officer at the contact details provided below.

5.2. Please note that a reasonable fee may be charged for an access request. If so, we will inform you of the fee before processing your request.

5.3. We will respond to your access request as soon as reasonably possible. Should we not be able to respond to your access request within 30 days after receiving your access request, we will inform you in writing within 30 days of the time by which we will be able to respond to your request. If we are unable to provide you with any personal data or to make a correction requested by you, we shall generally inform you of the reasons why we are unable to do so (except where we are not required to do so under the PDPA).

5.4. Please note that depending on the request that is being made, we will only need to provide you with access to

the personal data contained in the documents requested, and not to the entire documents themselves. In those cases, it may be appropriate for us to simply provide you with confirmation of the personal data that the Company has on record, if the record of your personal data forms a negligible part of the document.

6. PROTECTION OF PERSONAL DATA

6.1. To safeguard your personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption and the use of privacy filters to secure all storage and transmission of personal data by us, and disclosing personal data both internally and to our authorized third-party service providers and agents (e.g., tax agents, payroll agents, insurance brokers, insurers) only on a need-to-know basis.

6.2. You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

7. ACCURACY OF PERSONAL DATA

We generally rely on personal data provided by you (or your authorized representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing or via email at the contact details provided below.

8. RETENTION OF PERSONAL DATA

8.1. We may retain your personal data for as long as it is necessary to fulfil the purposes for which they were collected, or as required or permitted by applicable laws.

8.2. We will cease to retain your personal data or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the personal data were collected and are no longer necessary for legal or business purposes.

9. Disclosure of Personal Data to Third Parties

9.1. We shall not disclose your personal data to any third parties without first obtaining your consent permitting us to do so, or unless any such disclosure is permitted under any of the statutory exemptions under the Act.

9.2. In this respect, please note that we may disclose your personal data to third parties without first seeking your consent, if such disclosure is either required or permitted under the Act, including without limitation, if the disclosure is required by law and/or regulations, or if there is an emergency.

9.3. For such third-party processors, PALO-IT shall undertake appropriate due diligence and enter an agreement that complies with the PDPA's requirements.

10. TRANSFERS OF PERSONAL DATA OUTSIDE OF SINGAPORE

We generally do not transfer your personal data to countries outside of Singapore. However, if we do so (e.g., for visa applications, internal mobility etc.), we will obtain your consent for the transfer to be made and will take steps to ensure that your personal data continues to receive a standard of protection that is at least comparable to that provided under the PDPA.

11. Administration and Management of Personal Data

11.1. We shall take appropriate measures to keep your personal data accurate, complete, and updated. This includes taking appropriate precautions and preventive measures to ensure that your personal data is adequately protected and secured. Appropriate security arrangements shall be taken to prevent any unauthorized access, collection, use, disclosure, copying, modification, leakage, loss, damage and/or alteration of your personal data.

11.2. We shall also take reasonable efforts to ensure that the personal data in our possession or under our control is destroyed 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 such personal data.
- Retention is no longer necessary for any other legal or business purposes.

11.3. Our websites may contain links to other websites not maintained by PALO-IT. Such third-party websites are subject to their own data protection and privacy practices, and you are encouraged to examine the data protection policies of those websites.

12. Direct marketing

PALO-IT shall ensure that it has appropriate consent from individuals to send them direct marketing communications. When a data subject exercises their right to object to direct marketing, such requests must be

honoured promptly.

13. DATA PROTECTION OFFICER

You may contact our Data Protection Officer if you have any inquiries or feedback on our personal data protection policies and procedures; or if you wish to make any request, in the following manner:

Name: Jessica Dourcy

Email Address: jdourcy@palo-it.com

Contact No.: +65 6220 9908

11 Beach Road #06-01, Singapore 189675

14. EFFECT OF POLICY AND CHANGES TO POLICY

14.1. This Policy applies in conjunction with any other policies, notices, contractual clauses, and consent clauses that apply in relation to the collection, use and disclosure of your personal data by us.

14.2. We may revise this Policy from time to time with prior notice. You may determine if any such revision has taken place by referring to the date on which this Notice was last updated. Your continued employment and participation in our recruitment process constitute your acknowledgment and acceptance of such changes.

Frequently Asked Questions

1. General

What is personal data'?

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. For more information, please visit Personal Data Protection Commission.

Is there any type of data that is not covered under the PDPA?

All non-personal data (such as statistics, numbers and other information that cannot be linked back to an individual) and business contacts are not covered under PDPA. For more information, please visit Personal Data Protection Commission.

Are the rights of a child covered under the PDPA?

For any child below 13 years of age, the rights to consent, access and correction can only be granted by their guardians.

2. Collection, Use & Disclosure

How does Pal-IT obtain my consent for collecting, using, or disclosing my personal data?

You may have given your consent when you signed up for our services:

- via any legal contract
- when you sign up a form, accepting the privacy notice

How do I withdraw consent from Palo-IT to collect, use and/or disclose my personal data?

You may request to withdraw your consent sending an email to sg-dpo@palo-it.com. Your request for withdrawal of consent for all modes will take effect within 30 days. Please note that the use of your personal data may be essential in order for us to provide the product/service which you have signed/subscribed.

Am I able to reinstate my consent after I have withdrawn it?

Yes, you may do so sending an email to sg-dpo@palo-it.com.

3. Access & Correction

Can I access the personal data that Palo-IT has of me?

Under the PDPA, you have the right to request access to your personal data that we have sending an email to sg-dpo@palo-it.com.

Do I need to pay for accessing my personal data with Singtel?

Depending on the type of personal data that you have requested for, a fee may be charged to cover our costs for providing such data. No fee will be charged when you access your personal information over the Internet or when making basic inquiries.

Can I submit a request for access to personal data on behalf of someone else?

You may request for access to personal data on behalf of someone else only if you obtain and are able to produce documents of proof of his/her authorisation. These documents include:

- Copy of NRIC of the person authorising the access
- Copy of NRIC of the person being authorised to access the data
- Letter of authorisation signed by the person authorising the access
- Any other supporting documents where applicable