PERSONAL DATA PROTECTION POLICY OF NETRUST PTE LTD

1. INTRODUCTION

1.1 NETRUST PTE LTD ("Netrust") respects the right of individuals to protect their personal data. Netrust is committed to protect the privacy of every individual's personal data in accordance with its obligations under the Personal Data Protection Act 2012 ("**PDPA**").

1.2 To comply with our obligations under the PDPA, we have produced this Personal Data Protection Policy ("**Policy**"). This Policy sets out what we must do when any personal data of an individual is collected, used or disclosed and it also seeks to provide general guidance as to how to collect, handle, store or transmit personal data that we may receive in the course of administering the affairs of the Company.

1.3 This Policy applies to all personnel of Netrust. All personnel of Netrust must familiarize themselves and comply with the obligations, policies and practices set out in this Policy.

1.4 Compliance with the PDPA is important, because a failure to observe the obligations under the PDPA could potentially expose the Company to complaints, criminal charges and/ or bad publicity. Any failure by personnel of the Company to comply with the PDPA may lead to disciplinary action for serious or repeated breaches and/ or a report being made to the Police, the Personal Data Protection Commission and any other relevant government authority.

OVERVIEW OF THE PDPA

2. The PDPA came into effect on 2 January 2013 with the main personal data protection provisions coming into force on 2 July 2014.

3. Purpose

3.1 The PDPA is concerned with the protection of "Personal Data", which is defined as any data, whether true or not, about an individual who can be identified from that data and other information that an organisation has access to. The PDPA seeks to balance the rights of an individual to protect his/ her personal data and the need of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

4. Business Contact Information

4.1 The PDPA does not apply to "Business Contact Information", such as an individual's name, position or title, business telephone number and fax number, business address, business email address and any other similar information about the individual, which was given for commercial purposes or for a non-personal purpose.

4.2 However, if a person gives his Business Contact Information to Netrust to receive goods or services from the Company for his personal purposes (in other words, he/ she wants Netrust to contact him/ her at his/ her office rather than his/ her home), then the business contact information of that person will be personal data for the purposes of the PDPA.

OBLIGATIONS UNDER THE PDPA

5. Consent for Collection, Use or Disclosure of Personal Data

5.1 We will obtain the consent of our customers and subscribers (collectively "**Subscribers**") before we collect use or disclose their personal data. In obtaining consent, we will use reasonable efforts to ensure that the Subscriber is advised of the identified purposes for which his/ her personal data is being collected, used or disclosed. Purposes will be stated in a manner that can be reasonably understood by the Subscriber.

5.2 We will seek consent to use and disclose personal data at the same time as we collect the personal data. If we intend to use or disclose the personal data for a new purpose that was not previously identified, we will seek consent to use and disclose the personal data before it is used or disclosed for the new purpose.

5.3 We will collect personal data directly from Subscribers, but we may also collect personal data from other sources including relatives or personal references or other third parties provided they have the right to disclose such personal data.

5.4 We will limit the type of personal data collected to that which is necessary for the purposes that we have identified.

5.5 A Subscriber may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. A Subscriber may contact us for more information regarding the implications of withdrawing consent.

5.6 In certain circumstances, personal data can be collected, used or disclosed without the consent of the individual. For example:

(a) the collection, use or disclosure is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection, use or disclosure cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent, such as when the individual is seriously ill or mentally incapacitated;

(b) the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(c) the collection, use or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;

(d) the collection, use or disclosure is necessary for evaluative purposes;

(e) the personal data was provided to Netrust by another individual to enable Netrust to provide a service for the personal or domestic purposes of that other individual.

6. Notification of Purpose

6.1 We will identify the purposes for which we collect, use or disclose personal data on or before we collect, use or disclose the personal data of Subscribers. Upon receipt of the personal data, we will use or disclose the personal data only for the identified purpose and for purposes that a reasonable person would consider appropriate in the circumstances.

6.2 As an organisation, we generally collect, use and disclose personal data for the following purposes:

(a) To identify our customers and subscribers to Netrust;
(b) To manage the administration and operations of Netrust;
(c) To establish and maintain responsible relationships among Subscribers; and
(d) To meet our legal and regulatory obligations.

6.3 When personal data that has been collected is to be used or disclosed for a purpose not previously notified, the new purpose will be notified to Subscribers prior to use. Unless the new purpose is permitted or required by law, consent will be required before the personal data will be used or disclosed for the new purpose.

7. Use of Existing Personal Data

7.1 Personal data collected prior to 2 July 2014, when the main provisions of the PDPA on the protection of personal data came into force, can continue to be used or disclosed but only for the purpose that the personal data was originally collected, unless a Subscriber has withdrawn his/ her consent for such continued use or disclosure of his/ her personal data.

7.2 If there is a new purpose for the use or disclosure of existing personal data, a fresh consent has to be obtained from the Subscribers for this new purpose.

8. Disclosure of Personal Data

8.1 Generally, only those with a need to know or whose duties or services reasonably require access to personal data are granted access to personal data about the Subscribers.

8.2 As an accredited Certificate Authority in Singapore, we may, however, disclose personal data of the Subscribers to the relevant Government authorities as required by law.

9. Access to Personal Data

9.1 Upon receipt of a request from a Subscriber, we will provide the Subscriber with a reasonable opportunity to review the personal data that we have about the Subscriber in our possession or under our control. Personal data will be provided within a reasonable time and at minimal cost to cover administrative expenses.

9.2 Upon receipt of a request from a Subscriber, we will provide an account of the use and disclosure of the personal data of the Subscriber. In providing an account of disclosure, we will provide a list of the organisations to which we may have disclosed personal data about the Subscriber.

9.3 In certain situations we may not be able to provide access to all of the personal data we hold about a Subscriber; for instance:

(a) If doing so would likely reveal personal data about another individual or could reasonably be expected to threaten the life or security of another individual;
(b) If doing so would reveal any confidential information;
(c) If the information is protected by legal privilege;
(d) If the information was generated in the course of a formal dispute resolution process; or
(e) If the information was collected in relation to the investigation of a contravention of a law or a breach of an agreement.

9.4 In such a case, we will provide the reasons for denying access to the personal data.

10. Accuracy and Correction of Personal Data

10.1 We will endeavor to ensure that the personal data collected will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Ensuring that the personal data that we possess is sufficiently accurate, complete and up-to-date will help minimize the possibility that inappropriate decisions are being made based on inaccurate or incomplete or outdated information.

10.2 We will promptly correct or complete any personal data found to be inaccurate or incomplete. Upon receipt of a request from a Subscriber to correct or update his/her personal data, we will promptly correct or update his/ her personal data.

10.3 Where we are not able to confirm the accuracy or completeness of a Subscriber's personal data (such as those Subscribers who have emigrated or who are no longer contactable), a note will be made against that Subscriber's personal data of potential unresolved differences.

10.4 Where appropriate, we will inform third parties having access to the personal data in question of any amended personal data or the existence of any unresolved differences.

11. Transfer of Personal Data Outside of Singapore

11.1 We will protect personal data disclosed to third parties by contractual or other means stipulating the purposes for which it is to be used and the necessity to provide a comparable level of protection.

11.2 We will not transfer any personal data to any organisation located in a country or territory outside Singapore unless that other organisation is subject (whether by way of legislation or contractual arrangement) to obligations of protection of personal data that are comparable to those under the PDPA.

12. Security

12.1 We have the responsibility under the PDPA to make reasonable security arrangements to protect the personal data that we possess or control to prevent unauthorized access, collection, use, disclosure or similar risks.

12.2 We will use appropriate security measures to protect personal data against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction, regardless of the format in which the personal data is held.

12.3 We operate close circuit television (CCTV) cameras in Netrust premises for security and operational purposes. Except for security purposes, we do not use these CCTV cameras to identify an individual personally.

13. Retention and Destruction

13.1 We will keep personal data only as long as it remains necessary or relevant for the identified purposes or as required by law.

13.2 Once the personal data in our possession or control is no longer necessary for administrative or legal purpose, we will destroy or erase the personal data or remove the means by which the personal data can be associated with particular individuals (such as by way of anonymizing the personal data).

14. Complaints

We will attend to and investigate any complaints concerning any possible breach of this Policy. If a complaint is found to be justified, we will take appropriate measures to resolve the complaint including, if necessary, amending our policies and procedures. The complainant will be informed of the outcome of the investigation regarding his/ her complaint.

15. Handling of Personal Data of Company Staff

15.1 The personal data of Netrust staff, whether permanent or temporary, will be used only for purposes connected with their employment with Netrust and for as long a period as is necessary following the termination of their employment.

15.2 We value the privacy of our Company staff and shall process the personal data of our Company staff in a fair and lawful manner. We will endeavour to comply with the obligations under the PDPA on the use of personal data in an employer-employee relationship.

15.3 From time to time, we may need to disclose some information held about Company staff to government agencies, such as the Ministry of Manpower and the Central Provident Fund Board, and other relevant third parties, such as insurers, medical clinics and hospitals, solely for purposes connected with managing the employment of Company staff and providing for his/ her welfare during his/ her employment with Netrust.

16. Consequences of Non-Compliance

16.1 Failure to comply with the provisions of the PDPA may expose Netrust to an investigation by the Personal Data Protection Commission (the "**PDPC**") of the non-compliance.

16.2 If the PDPC is satisfied that the Company is not complying with its obligations under the PDPA, the PDPC may give the Company such directions as it thinks fit in the circumstances, which may include directions to:

(a) stop collecting, using or disclosing personal data in contravention of the PDPA;
(b) destroy personal data collected in contravention of the PDPA;
(c) provide access to or correct the personal data in such manner and within such time as the PDPC may specify.

17. Appointment and Duties of the Data Protection Officer

17.1 Netrust is required, as part of its compliance with the PDPA, to designate at least one person as its Data Protection Officer ("**DPO**").

17.2 It should be noted that the designation of a DPO does not relieve Netrust of its legal obligations under the PDPA.

17.3 The DPO is responsible for ensuring that the Company complies with the PDPA. The DPO would keep fully up to date with the requirements of the PDPA and ensure that all personnel who handle personal data are fully aware of these requirements.

17.4 Where appropriate, the DPO may delegate some of his responsibilities as DPO to other individuals to ensure that Netrust complies with the PDPA.

17.5 In addition to ensuring that the Company complies with the PDPA, the DPO is also responsible for dealing with queries and requests from individuals in relation to the Company's data protection policies and practices.

18. Contact our Data Protection Officer

18.1 If a Subscriber or an employee of Netrust believes that information we hold about him is incorrect or out of date, or if an individual has concerns or further queries about how we are handling his personal data, or any problem or complaint about such matters, please contact the Data Protection Officer at DPO@netrust.net.