SECTION ONE: INTRODUCTION

I. OBJECTIVES OF POLICY

1. The *Personal Data Protection Act* (No. 26 of 2012) ("***PDPA***") has imposed new standards on organisations for the collection, use and disclosure of personal data in Singapore.

2. The objective of this Personal Data Protection Policy ("***Policy***") is to provide employees of New Silkroutes Group Limited and its Group of Companies ("***NSG***") with instructions for the collection, use and disclosure of personal data in compliance with the PDPA.

3. This Policy will also help NSG achieve the ancillary benefits of personal data protection compliance. It will increase customer confidence and trust in NSG, enhance the image of NSG, improve information management processes, and institute a culture of data protection awareness among NSG employees. If necessary, individual departments should use this Policy to formulate department-specific standard operating procedures, taking their own data-related activities into account.

4. A failure to comply with this Policy could expose NSG to enforcement action by the Personal Data Protection Commission ("***PDPC***"), including the imposition of financial penalties of up to S$1 million. In addition, there may be negative publicity from any breach that is made public. For individuals, obstructing PDPC officers (e.g. in the course of their investigations) or providing false statements could attract a fine of up to S$10,000 and/or imprisonment for up to 12 months. Compliance with this Policy will help NSG and its employees avoid such negative consequences.

II. SCOPE OF POLICY

5. This Policy applies to all NSG employees (whether on a part-time, temporary or full-time basis), interns and trainees ("***Employees***") working at or attached to NSG who are granted access to and/or process personal data on behalf of NSG. A violation may result in disciplinary action including termination of employment and/or contract.

6. This Policy does not form part of the formal contract of employment for Employees but it is a condition of employment that Employees shall abide by policies made by NSG from time to time. Any non-compliance with the Policy can result in disciplinary action being taken against the offending Employee.

7. This Policy may be updated from time to time. Employees should familiarise themselves with this Policy and any subsequent versions. This Policy is not intended to supersede or override other policies relating to the handling of personal data. Employees should continue to observe all other policies pertaining to the handling of personal data including any applicable confidentiality or secrecy obligations.

SECTION TWO: OVERVIEW OF LEGISLATION

I. OVERVIEW

8. The PDPA governs the collection, use and disclosure of personal data by organisations, and recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data in appropriate circumstances.

II. DEFINITIONS

9. "***Personal data***" refers to information, whether true or not, about an individual who can be identified from (a) that data; or (b) from that data and other information which the organisation is likely to have access to. It covers all forms of personal data, whether in electronic or non-electronic form.

    - Personal data under the PDPA may include an individual's full name, NRIC or FIN number, passport number, photograph or video image, mobile telephone number, personal e-mail address, thumbprint, name and residential address/phone number, name and age/date of birth, etc.

10. "***Individual***" means a natural person, whether living or deceased.

11. "***Business contact information***" refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, unless the personal data was provided by the individual solely for his/her personal purposes.

III. EXCLUSIONS

12. The PDPA does not apply to business contact information. Employees are not required to obtain consent before collecting, using or disclosing any business contact information or comply with any other obligation in the PDPA in relation to business contact information.

13. Whether data is considered business contact information depends on the purpose for which such contact information is provided. For example, an individual may provide work-related contact information solely for personal purposes, while a sole proprietor may provide personal contact details for business purposes.

IV. COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

14. Employees cannot collect, use or disclose personal data about an individual unless: (a) the individual gives, or is deemed to give, his/her consent under the PDPA to the collection, use or disclosure; or (b) the collection, use or disclosure, without the consent of the individual, is required or authorised under the PDPA or any other written law.

15. Consent is valid if Employees have provided the individual with information regarding: (a) the purpose for the collection, use or disclosure of the personal data before collecting the personal data; (b) any other purpose regarding the use or disclosure of personal data not otherwise told to the individual; and (c) on request by the individual,

the business contact information of a person who is able to answer the individual's questions about the collection, use or disclosure on behalf of NSG.

16. Consent for the collection, use or disclosure of personal data by NSG is deemed given for a specific purpose if: (a) the individual voluntarily provides the personal data to Employees for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data.

17. No Employee shall attempt to obtain consent for collecting, using or disclosing data by: (a) providing false or misleading information with respect to the collection, use or disclosure of the personal data; or (b) using deceptive or misleading practices. A breach of this paragraph may result in the relevant Employee facing disciplinary action and/or termination by NSG.

18. If an individual chooses to withdraw his/her consent for the collection, use or disclosure of personal data, he/she must complete and sign the Personal Data Access/Correction/Withdrawal Request Form in ***Appendix 1***. An Employee shall inform the individual of the likely effect(s) of such a withdrawal. The Employee shall not prohibit the individual from withdrawing his/her consent to the collection, use or disclosure of personal information.

19. Employees may only collect, use or disclose personal data for the purposes that: (a) a reasonable person would consider appropriate in the circumstance; and (b) Employees inform the individual about.

20. Personal data can be collected, used and disclosed without consent in certain specific circumstances set out in the Second, Third and Fourth Schedules of the PDPA set out in ***Annex 3***. Some of the relevant exceptions include:

- Where the personal data collected from an Employee is necessary for the purpose of managing or terminating the employment relationship between NSG and that Employee; and

- Where the personal data collected from an Employee is necessary for evaluative purposes**.**

Employees are strongly encouraged to check with the Data Protection Officer ("***DPO***") if they are unsure whether any of the exceptions to collecting, using or disclosing personal data without consent in to ***Annex 3*** are applicable to the situation at hand.

V. ACCESS TO AND CORRECTION OF PERSONAL DATA

21. Subject to paragraph 22, upon the request of an individual, Employees may be required to provide the individual with: (a) the individual's personal data in the custody or under the control of NSG; and (b) information about the ways in which such personal data referred to in (a) has been or may have been used by NSG within one (1) year before the date of the request.

22. Employees shall not disclose personal data and other information to the requesting individual if such disclosure could: (a) reasonably be expected to reveal personal data about another individual; or (b) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his/her identity. Other exceptions to this access and correction requirements may be found in the Fifth and Sixth Schedule of the PDPA

as set out in ***Annex 4***. Employees are encouraged to consult the DPO if they are unsure if one of the exceptions applies.

23. Unless NSG is satisfied on reasonable grounds that a correction should not be made, the DPO should correct the personal data as soon as is practicable, and send the amended personal data to: (i) every organisation to which the personal data was disclosed by NSG within one (1) year before the date the amendment was made; or (ii) if the individual consents, only to specific organisations to which the personal data was disclosed within one (1) year before the date of the amendment.

24. If the DPO decides that no correction should be made, the DPO shall annotate the reason(s) for not granting such correction request with a note of the request.

25. To make a request to access, correct or update personal data retained by NSG, the individual must submit a Personal Data Access/Correction/Withdrawal Request Form found in ***Appendix 1*** to the DPO.

VI. ACCURACY OF PERSONAL DATA

26. Employees shall make reasonable effort to ensure that the personal data collected by or on behalf of NSG is accurate and complete, if the personal data: (a) is likely to be used by NSG to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by NSG to another organisation.

27. When Employees collect personal data on behalf of NSG, they should ensure that the collected personal data is accurate and complete. Personal data may be considered inaccurate if it is incorrect or not updated. Personal data may also be considered incomplete if a relevant part is missing.

28. Every department in NSG should take reasonable steps to verify that the data they collect is complete and up-to-date at the point of collection.

29. If an Employee is uncertain as to the steps which he/she may need to take to ensure that the personal data is accurate and complete during the collection of the data, he/she should check with the DPO.

VII. PROTECTION OF PERSONAL DATA

30. Employees shall make reasonable security arrangements to protect the personal data in its custody or under its control and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks in respect of such data. In particular, the DPO shall ensure that all employees involved with the collection, use or disclosure of personal data of customers and/or suppliers shall surrender all the personal data collected by them via any unauthorised means, e.g., collected and stored in their personal hand phones. The DPO shall also take steps to ensure its employees refrain from collecting personal data via unauthorised methods in the future.

31. These security arrangements can be administrative, physical or technical measures or a combination of these. There is no one-size-fits-all solution. Employees are encouraged to check with the DPO when deciding which measures to adopt.

32. The measures adopted should be reasonable and appropriate in the circumstances, depending on the nature of the personal data, the form in which the personal data has

been collected, e.g. physical or electronic, and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

33. If any Employee feels that any personal data is at risk, they should immediately bring the matter to the attention of the DPO.

VIII. RETENTION OF PERSONAL DATA

34. NSG is not allowed to retain personal data for an indefinite length of time. Unless specific retention periods are necessary, no department in NSG shall retain personal data for a period of time exceeding 6 years.

35. Employees should destroy documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, when it is reasonable to assume that: (a) the purpose for which that personal data was collected is no longer being served by retention of personal data; and (b) retention is no longer necessary for legal or business purposes.

36. Examples of acceptable purposes for retention of personal data include: carrying out business operations, generating annual reports or performance forecasts, auditing, ongoing legal action, or complying with laws or regulations.

37. Once the retention period has expired relative to an individual's personal data, Employees should either (a) destroy or dispose of the personal data; or (b) anonymise the personal data, such that it is no longer possible to associate the personal data with any particular individual.

38. In certain circumstances, however, the personal data may instead be: (a) returned to the individual concerned; or (b) transferred to another party, provided the individual has given express written instructions. In these circumstances, Employees should obtain prior written approval from the DPO before returning or transferring such personal data to the relevant individual concerned.

39. It is recommended that each NSG department ought to take the following action:

- Conduct regular checks on personal data retained (at least once a year);
- Obtain clearance/approval from the DPO as to how the data shall be destroyed, anonymised, returned or transferred (as set out in the preceding paragraphs); and
- Comply with this Policy and all instructions by the DPO in respect of the personal data which is no longer retained.

IX. TRANSFER OF PERSONAL DATA OUTSIDE OF SINGAPORE

40. The PDPA requires that before transferring any personal data out of Singapore, Employees must ensure that a comparable standard of protection shall be provided to the personal data by the receiving entity that is comparable to the standard of protection required under the PDPA. The Personal Data Protection Regulations 2014

requires Employees to take appropriate steps to ascertain whether, and ensure that, the receiving entity is bound by contractual agreements, binding corporate rules, or any other legally binding instrument to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

41. When an Employee is transferring personal data out of Singapore for the first time, he/she should check with the DPO on how to comply with the PDPA requirements before making the transfer.

SECTION THREE: BUSINESS

I. COLLECTION OF PERSONAL DATA

Consent Required

42. All Employees shall only collect, use or disclose personal data about an individual when the individual gives or is deemed to have given, his/her consent under the PDPA to the collection, use or disclosure as the case may be, or when the collection, use or disclosure without the consent of the individual is required or authorised under the PDPA or any other written law.

Provision of consent

43. An individual has not given consent under the PDPA for the collection, use or disclosure of personal data about the individual by an Employee for a purpose unless the Employee informs the individual of the purpose for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; and any other purpose of the use or disclosure of the personal data which the individual has not been informed before the use or disclosure of the personal data for that purpose; and the individual provides his consent for that purpose in accordance with the PDPA.

44. On request by the individual, all Employees must also provide the business contact information of the DPO or any other person who is able to answer on behalf of NSG the individual's questions about the collection, use or disclosure of the personal data.

45. In collecting personal data from Individuals, Employees must ensure that consent is given in accordance with the PDPA, in the manner set out above.

Deemed Consent

46. An individual may be deemed to have provided consent to NSG to collect, use and/or disclose his/her personal data for a specific purpose if: (1) the individual voluntarily provides his/her personal data to NSG for that purpose, and (2) it is reasonable that the individual would do so.

47. The onus is on NSG to ensure that the individual is aware of the purpose for which his/her personal data would be collected, used or disclosed. Consent would not be deemed to have been given where the individual cannot reasonably be expected in the circumstances to have provided his/her personal data for a purpose.

48. Where it is not clear whether the deemed consent provision would apply, it is recommended that Employees, as far as possible, obtain consent from the individual as this would avoid disputes where an individual claim that he/she did not consent to the collection of his/her personal data for a purpose and that he/she did not voluntarily provide data for that purpose.

49. Before relying on deemed consent to collect, use or disclose an individual's personal data for various purposes, Employees are encouraged to check with their respective departments and the DPO whether such reliance is acceptable in the circumstances, and whether the particular individual has withdrawn his/her consent.

Closed-circuit television cameras ("CCTVs")

50. NSG does not need to obtain consent from individuals when their personal data (image and/or video footage) is captured on the CCTVs installed in NSG's premises for security purposes. However, as a matter of good practice, signs should be placed at premises informing individuals that the premises are under CCTV surveillance, and clearly stating the use and purpose of such surveillance.

51. These notices should be placed at points of entry or at prominent locations in a venue to provide individuals with sufficient awareness of the existence of the CCTVs, though they do not have to reveal the exact location of the CCTVs.

52. In general, Employees may collect, use or disclose an individual's image and video footage captured by CCTVs without consent from the individual in question if it falls within one the exceptions in the Second, Third or Fourth Schedule of the PDPA respectively. For example, consent is not required where the CCTV footage is necessary to conduct investigations, including internal and police investigations, or legal proceedings.

Events and Functions

53. At events, an Employee may be appointed to take photos and/or film videos. These photos and/or videos may be recorded in the Employee's personal mobile phone or camera for the purposes of event coverage and documentation. If a professional photographer or videographer from an external company is engaged to take pictures and/or record footage of the event, the external company has to sign the Non-Disclosure and Security Awareness Undertaking (Third Parties) found at ***Appendix 2***. If the external company chooses not to sign the form, Employees can alternatively request for it to give NSG an undertaking to indemnify NSG for any losses arising from their breach of the PDPA.

54. Regardless of the event or function, consent should be first obtained from the guests before their photo is taken or their person recorded on video. The purposes for which Employees may use these photos or videos shall be limited to the specified purpose(s) provided to the guests when obtaining their consent.

55. Although it is possible to obtain this consent through the photographer/videographer verbally asking each guest for permission, it may be more convenient for Employees to obtain deemed consent by providing notice to the guests. This can be done by informing the guests in attendance of the use of photos and videos taken during the event either within the invitation or on signage placed on the registration tables. In this way, the guests would be deemed to have consented to having their photos taken and their person filmed.

SECTION FOUR: HUMAN RESOURCE

I. JOB APPLICANTS

56. When an individual voluntarily provides his/her personal data to NSG in the form of a job application, NSG has obtained deemed consent to collect, use and disclose that individual's personal data for the purpose of assessing his/her job application. Correspondingly, NSG may only collect, use and/or disclose such data for purposes that a reasonable person would consider appropriate in the circumstances.

II. EXISTING EMPLOYEES

57. An exception to the consent obligation under the PDPA is the reasonable collection of personal data from an Employee for the purpose of managing or terminating the employment relationship between NSG and that Employee.

58. All existing Employees shall be made aware of their responsibilities in connection with the PDPA mentioned in this Policy through the company Microsoft Teams General Folder.

59. Furthermore, the consent form seeks to facilitate NSG's fulfilment of all its foreseeable notification and consent obligations under the PDPA at once, bypassing the need for NSG to distinguish between the obligations they are subject to for each type of personal data collected from employees. The form shall also enable NSG to have proper records of the purposes for which it has collected the personal data in this document.

60. This exercise shall be administered by the Human Resource ("***HR***") Department. Subsequently, new Employees shall sign employment contracts which shall include a data protection and general confidentiality clause.

61. A breach of the PDPA and/or any provision in this Policy by any Employee shall result in his/her facing disciplinary action and/or possible termination of employment.

62. All Employees, past employees, and/or prospective employees who want to access, correct or update their personal data retained by NSG will need to contact the DPO and make their request by submitting the Personal Data Access/Correction/Withdrawal Request Form found at ***Appendix 1***.

63. The DPO shall respond to all requests within fourteen (14) working days of receipt of a written request, unless there is a good reason for a delay. Where appropriate, the DPO shall give such reason(s) for delay in writing to the individual who is making the request.

SECTION FIVE: INFORMATION TECHNOLOGY

64. Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking. Password length must be at the very minimum 6 characters. Employees shall change their passwords every 90 days.

65. Contractors, consultants, third party service providers hired by NSG that have access to PCs should provide an undertaking in the form of the Non-Disclosure and Security Awareness Undertaking (Third Parties) found at ***Appendix 2***, before commencing work and/or services for NSG.

66. Reception staff should ensure that visitors to NSG's offices and any other unauthorised persons are unable to view personal or confidential information whether retained on paper or information displayed on computer monitors at the reception area.

67. Employees should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally stored computerised databases and files containing personal data.

68. Employees should ensure that their computers are logged off or “locked” when left unattended for any period of time

69. While Employees in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data.

70. Employees working with personal data shall be informed by their managers of the purposes for which the data is being processed and the legitimate parties either within or outside NSG to whom the data, either in whole or in part, may be disclosed or transferred. Personal information must not be disclosed orally, or in writing, or via web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

71. Where personal data is transferred between Employees or departments within NSG in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied.

72. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information stored on the device.

73. In general, no personal data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or friends should be refused unless consent is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law. Employees should never discuss matters, whether existing or potentially new matters, in public or common areas.

74. Requests for the disclosure of personal data from the police, government bodies or other official agencies should be investigated sufficiently to verify the authenticity of the requests and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

SECTION SIX: E-MAIL AND PRIVACY POLICY

I. E-MAIL DISCLAIMER

75. NSG's e-mail disclaimer shall state:

> Disclaimer: This e-mail, which represents solely the views of its author, is confidential to the e-mail addressee and may contain copyright and/or legally privileged information. No-one else may read, print, store, copy, forward or act in reliance on it/any attachment(s). Please e-mail the sender if you receive this in error. No responsibility shall be accepted for any damage caused by this e-mail/attachment(s). New Silkroutes Group Limited has taken the necessary steps to comply with the *Singapore Personal Data Protection Act* (No. 26 of 2012) and takes all reasonable care to prevent any unauthorised access to any personal data you may submit to us via this e-mail.

II. NSG'S PRIVACY POLICY

76. The NSG's Privacy Policy attached at ***Annex 1*** is to be included at NSG and its Group of Companies' websites. The Privacy Policy is made accessible to web users and serves as a notice for obtaining deemed consent from them to collect, use and disclose their personal data.

SECTION SEVEN: RETENTION AND DISPOSAL OF PERSONAL DATA

77. Employees are required to cease to retain documents containing an individual's personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer served by its retention, and retention is no longer necessary for legal and business purposes.

78. Different types of personal data shall be retained for varying periods of time. The PDPA does not prescribe a fixed duration of time for which an organisation can keep personal data, but instead assesses the retention period based on a standard of reasonableness, with regard to the purposes for which the personal data was collected, and other applicable legal or specific industry-standard requirements. For NSG, the different retention periods are set out in Personal Data Retention Policy attached at ***Annex 2***.

79. It is understood that NSG shall retain an Employee's personal data for a period of time following their departure from NSG, mainly for legal reasons, but also for other purposes such as being able to provide references and recommendations. NSG may also require the personal data for regulatory and compliance reasons, for example responding to requests from the government authorities and public agencies, including but not limited to, the Central Provident Fund, Inland Revenue Authority of Singapore, or Ministry of Manpower.

80. Employees whose work involves the collection, use and disclosure of personal data, whether in electronic or paper format, must take personal responsibility for its secure storage.

81. Personal data should never be stored in Employees' homes, whether in paper or electronic form, on laptop computers, or other personal portable devices or at other remote sites.

SECTION NINE: DATA PROTECTION OFFICER

I. IMPLEMENTATION AND DISSEMINATION OF POLICY

82. The DPO is responsible for ensuring compliance with this Policy.

83. Further, the primary responsibility for the implementation of the Policy rests with the DPO, though all Employees are also obliged to adhere to, support and implement this Policy.

84. If an Employee finds that this Policy is inconsistent with any other NSG policy or obligation or if the Employee is aware that this Policy is not being followed in respect of any personal data, the DPO must be informed at **dpo@newsilkroutes.org**.

II. COMPLAINTS PROCEDURE

85. All complaints in relation to personal data shall be referred to the DPO.

86. The DPO shall endeavor to attend to any complaint and shall acknowledge receipt of the complaint/notification within fourteen (14) working days. Further contact shall be dependent upon the nature of the complaint.

87. The DPO shall respond within one (1) month from the date the complaint was acknowledged. The DPO may request that the complainant assists with any investigation that takes place, or answer any questions that the DPO may have regarding the complaint. In this regard, the DPO may also request a meeting with the complainant if necessary.

88. The DPO shall confirm his/her decision about the complaint in writing after completing its investigation.

ANNEXES

Annex 1 – Privacy Policy

New Silkroutes Group Limited and its Group of Companies ("**we**", "**our**", "**us**") value the information you have provided us or permitted us to collect. We strive to protect your privacy while providing you with the best service and experience we can provide. All such personal information in our possession is valued and is collected, used, disclosed and protected in accordance with the Singapore Personal Data Protection Act 2012 ("**PDPA**"). This Privacy Policy applies to all websites on which this Privacy Policy or a link to this Privacy Policy appears, as well as all our activities to the extent that you have been notified that such activities are subject to this Privacy Policy.

By visiting or using any of the websites on which this Privacy Policy or a link to this Privacy Policy appears, you are deemed to agree to the terms of this Privacy Policy. Please review this Privacy Policy carefully prior to visiting or using any such websites or otherwise providing any personal data.

If you wish to opt-out of this Privacy Policy, amend or remove any of your personal data in our possession, please read paragraph 6 below for the required procedure.

1. PERSONAL INFORMATION AND OTHER DATA WE COLLECT

Personal data as defined in the PDPA refers to data about an individual who can be identified from either that particular data, or from that data and other information which we have or are likely have access to. Personal data is collected where reasonably necessary for our functions and activities. Personal data that we may hold include the following:

(A) name, address and contact details;

(B) date of birth;

(C) NRIC number, FIN number, driver's licence, passport number, or work permit number;

(D) employment and income details;

(E) bank account details;

(F) details of services provided to an individual by us;

(G) details of an individual's dealings with us, including telephone records, email and online interactions;

(H) credit-related personal information;

(I) photos and CCTV recordings; and

(J) other personal data as may be provided by an individual from time to time.

Collection of personal data

Wherever possible, we will collect personal data directly from you. We will only collect, use and disclose personal data with your consent, your deemed consent or as may be otherwise permitted under the PDPA or other applicable laws.

In addition to the personal data you provide to us, certain information related to you that is not considered personal data under the PDPA may also be collected. We collect this information to improve our website. Such non-personal data may include information such as your IP address, the internet browser you use, details of your interaction with our website and other types of non-personal data.

Use of cookies

Cookies are small files which require user permission in order to be installed on a computer's hard drive. Cookies will only start to perform their functions after such permission is granted. By collecting and analysing data on the user's browsing patterns, cookies allow web applications to respond to the user as an individual by tailoring a web application's operations to the user's specific needs and preferences.

Permission for cookies is granted by default in most web browsers. You can however choose to disable this function in your browser's settings. This may prevent you from taking full advantage of our website.

We may use traffic log cookies to identify which pages are being used. This use is designed to assist us in gathering data on web page traffic. The gathered data is used only for statistical purposes and is removed from our database shortly after.

Overall, the data collected by the cookies is used for the purpose of improving your browsing experience on our website. Cookies do not grant us access to your computer or any information about you outside of your browsing activity on our website.

2. USE OF YOUR PERSONAL DATA

We collect personal data from our existing and prospective customers, business associates and employees for various reasons. Without limitation, these purposes include:-

(A) providing customer support;

(B) supplying you with information that is relevant to your existing relationship with us;

(C) processing your employment applications;

(D) for fraud prevention and detection; or

(E) in our sole discretion, in exceptional circumstances such as national emergency, security concerns, or other situations in which we deem that such disclosure is prudent.

We may, for the above purposes, contact you via mail, electronic mail, telephone, SMS, facsimile or other forms of communication through mobile applications. Should you wish to opt-out of our contact list for any reason, please refer to the below paragraph 6 for the relevant procedure.

3. SHARING YOUR PERSONAL DATA

In the course of providing our services and products to you, we may need to disclose your personal data with external organisations. The reasons for which we may disclose your personal data are set out under the paragraph 2 above. The possible parties we may share your personal data with include our group companies, our affiliates, partners, principals, third party service providers (for the purpose of providing us administrative or marketing support), and governmental or regulatory authorities. If any of our businesses are sold or transferred to another entity, your personal data may be transferred along with the business.

In the event that any of the above parties receiving your personal data are located or are operating outside of Singapore, we will take reasonable steps to ensure that the overseas recipient provides a standard of protection to your personal data so transferred that is comparable to the protection under the PDPA.

4. SECURITY

We will protect your personal data using industry standard precautions. While the transference of electronic data over the internet has inherent risks, we use reasonable precautions to ensure your personal data is not subject to unnecessary risks.

5. RETENTION

We will retain your Personal Data for as long as necessary in order to fulfil the purpose for which it was collected, or as required by the relevant laws.

6. ACCESS, UPDATE, WITHDRAWAL OF CONSENT

You must obtain, fill out, and submit to us a written request if you subsequently decide to request access of, update or withdraw your consent for us to collect, use and/or disclose your personal data. Please note that it may take up to 14 business days to attend to your request and an additional 30 business days for us to process your request.

7. RIGHTS TO AMEND THIS PRIVACY POLICY

We reserve the right to amend this Privacy Policy at any time. If material changes are made to this Privacy Policy, they will be posted on this page and date stamped. We encourage you to review this page periodically in order for you to stay notified of any changes.

Your continued use of this website and acceptance of our services after any changes to this Privacy Policy constitutes your consent to any such changes, to the extent such consent is not otherwise provided.

8. CONTACT US

If you have comments or questions about this Privacy Policy statement, or wish to obtain a form mentioned in paragraph 6, please contact our us at: **dpo@newsilkroutes.org**

Annex 2 – Personal Data Retention Policy

No.	Type of Personal Data	Suggested Retention Period	Comments
	Employees' Personal Data		
1	Completed employment application forms	2 years after departure of an employee	
2	Application forms of potential job applicants (including CVs, and resumes)	6 months after the receipt of the application form	
3	Employee files including record of service, evaluation(s), annual appraisal and assessment records	2 years after departure of an employee	
4	Records of promotion, transfer and bonus matters	2 years after departure of an employee	
5	Notes of disciplinary action/warning	2 years after departure of an employee	
6	Salary and overtime pay records	2 years after departure of an employee	
7	Employee insurance claims records	2 years after departure of an employee	
8	Employee benefit claims records	2 years after departure of an employee	
9	Annual leave records	2 years after departure of an employee	
10	Sick leave and hospitalisation records	2 years after departure of an employee	
11	Statutory maternity leave pay records and calculations	2 years after departure of an employee	
12	Statutory childcare leave pay records and calculations	2 years after departure of an employee	

13	Personal data of interns and temporary staff	2 years after departure of an employee	
14	Personal data of former employees / referrals	2 years after departure of an employee	
	Customers' Personal Data		
15	Photographs/videos from NSG events/functions	No prescribed retention period	
16	CCTV recordings; security	6 years after the date of recording; 6 years after the relevant security records	
	Patients' Records		
17	All patients' records	No longer than 6 years for non high risks patient & 6 years and longer for high risks patients. Patient is considered inactive having not been to the clinic in the last 3 years.	

Annex 3 – Collection Use and Disclosure of Personal Data without Consent

---

SECOND SCHEDULE

Section 17(1)

COLLECTION OF PERSONAL DATA WITHOUT CONSENT

1. *An organisation may collect personal data about an individual without the consent of the individual or from a source other than the individual in any of the following circumstances:*

(a) the collection is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

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

(c) the personal data is publicly available;

(d) the collection is necessary in the national interest;

(e) the collection 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;

(f) the collection is necessary for evaluative purposes;

(g) the personal data is collected solely for artistic or literary purposes;

(h) subject to paragraph 2, the personal data is collected by a news organisation solely for its news activity;

(i) the personal data is collected for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;

(j) the collection is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(k) the personal data is collected by a credit bureau from a member of the credit bureau to create a credit report, or by a member of the credit bureau from a credit report provided by the credit bureau to that member in relation to a transaction between the member and the individual;

(l) the personal data is collected to confer an interest or a benefit on the individual under a private trust or a benefit plan, and to administer such trust or benefit plan, at the request of the settlor or the person establishing the benefit plan, as the case may be;

(m) the personal data was provided to the organisation by another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual;

(n) the personal data is included in a document —

> (i) produced in the course, and for the purposes, of the individual's employment, business or profession; and

(ii) collected for purposes consistent with the purposes for which the document was produced;

(o) the personal data is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual;

(p) subject to the conditions in paragraph 3, the personal data —

(i) is collected by an organisation, being a party or a prospective party to a business asset transaction with another organisation, from that other organisation;

(ii) is about an employee, customer, director, officer or shareholder of the other organisation; and

(iii) relates directly to the part of the other organisation or its business assets with which the business asset transaction is concerned;

(q) the personal data was disclosed by a public agency, and the collection is consistent with the purpose of the disclosure by the public agency; or

(r) the personal data —

(i) was disclosed to the organisation in accordance with section 17(3); and

(ii) is collected by the organisation for purposes consistent with the purpose of that disclosure.

2. *In this paragraph and paragraph 1(h) —*

"broadcasting service" has the same meaning as in section 2 of the Broadcasting Act (Cap. 28);

"news activity" means —

(a) the gathering of news, or the preparation or compilation of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning —

(i) news;

(ii) observations on news; or

(iii) current affairs;

"news organisation" means —

(a) any organisation —

(i) the business of which consists, in whole or in part, of news activity carried out in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper; and

(ii) which, if the organisation publishes a newspaper in Singapore within the meaning of section 8(1) of the Newspaper and Printing Presses Act (Cap. 206), is required to be a newspaper company within the meaning of Part III of that Act; or

(b) any organisation which provides a broadcasting service in or from Singapore and holds a broadcasting licence granted under section 8 of the Broadcasting Act;

"newspaper" has the same meaning as in section 2 of the Newspaper and Printing Presses Act;

"relevant broadcasting service" means any of the following licensable broadcasting services within the meaning of the Broadcasting Act:

(a) Free-to-air nationwide television services;

(b) Free-to-air localised television services;

(c) Free-to-air international television services;

(d) Subscription nationwide television services;

(e) Subscription localised television services;

(f) Subscription international television services;

(g) Special interest television services;

(h) Free-to-air nationwide radio services;

(i) Free-to-air localised radio services;

(k) Subscription nationwide radio services;

(l) Subscription localised radio services;

(m) Subscription international radio services;

(n) Special interest radio services.

3.—(1) *The conditions in this paragraph shall apply if the personal data is collected under paragraph 1(p).*

(2) If the organisation is a prospective party to a business asset transaction —

(a) the personal data collected must be necessary for the organisation to determine whether to proceed with the business asset transaction; and

(b) the organisation and the other organisation must have entered into an agreement that requires the prospective party to use or disclose the personal data solely for purposes related to the business asset transaction.

(3) If an organisation enters into the business asset transaction with another organisation —

(a) the organisation shall only use or disclose the personal data collected for the same purposes for which the other organisation would have been permitted to use or disclose the data;

(b) if any of the personal data collected does not relate directly to the part of the other organisation or its business assets with which the business asset transaction entered into is concerned, the organisation shall destroy, or return to the other organisation, any such personal data; and

(c) the employees, customers, directors, officers and shareholders whose personal data is disclosed shall be notified that —

(i) the business asset transaction has taken place; and

(ii) the personal data about them has been disclosed to the organisation.

(4) If a business asset transaction does not proceed or is not completed, the organisation shall destroy, or return to the other organisation, all the personal data collected.

(5) In this paragraph and paragraph 1(p), "business asset transaction" has the same meaning as in paragraph 3(4) of the Fourth Schedule.

4. *For the avoidance of doubt, personal data disclosed before the appointed day in the circumstances and conditions set out in the Fourth Schedule shall satisfy paragraph 1(r), notwithstanding that section 17(3) was not in force at the time of the disclosure.*

THIRD SCHEDULE

Section 17(2)

USE OF PERSONAL DATA WITHOUT CONSENT

1. *An organisation may use personal data about an individual without the consent of the individual in any of the following circumstances:*

(a) the use is necessary for any purpose which is clearly in the interests of the individual, if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

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

(c) the personal data is publicly available;

(d) the use is necessary in the national interest;

(e) the use is necessary for any investigation or proceedings;

(f) the use is necessary for evaluative purposes;

(g) the personal data is used for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;

(h) the use is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(i) subject to the conditions in paragraph 2, the personal data is used for a research purpose, including historical or statistical research; or

(j) the data was collected by the organisation in accordance with section 17(1), and is used by the organisation for purposes consistent with the purpose of that collection.

2. *Paragraph 1(i) shall not apply unless —*

(a) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

(b) it is impracticable for the organisation to seek the consent of the individual for the use;

(c) the personal data will not be used to contact persons to ask them to participate in the research; and

(d) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

3. *For the avoidance of doubt, personal data collected before the appointed day in the circumstances and conditions set out in the Second Schedule shall satisfy paragraph 1(j) notwithstanding that section 17(1) was not in force at the time of the collection.*

FOURTH SCHEDULE

Sections 2, 17(3) and 21(4)

DISCLOSURE OF PERSONAL DATA WITHOUT CONSENT

1. *An organisation may disclose personal data about an individual without the consent of the individual in any of the following circumstances:*

(a) the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;

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

(c) subject to the conditions in paragraph 2, there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way;

(d) the personal data is publicly available;

(e) the disclosure is necessary in the national interest;

(f) the disclosure is necessary for any investigation or proceedings;

(g) the disclosure is to a public agency and such disclosure is necessary in the public interest;

(h) the disclosure is necessary for evaluative purposes;

(i) the disclosure is necessary for the organisation to recover a debt owed by the individual to the organisation or for the organisation to pay to the individual a debt owed by the organisation;

(j) the disclosure is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(k) the personal data is disclosed by a member of a credit bureau to the credit bureau for the purpose of preparing credit reports, or in a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual;

(l) the personal data about the current or former students of the organisation, being an education institution, is disclosed to a public agency for the purposes of policy formulation or review;

(m) the personal data about the current or former patients of a healthcare institution licensed under the Private Hospitals and Medical Clinics Act (Cap. 248) or any other prescribed healthcare body is disclosed to a public agency for the purposes of policy formulation or review;

(n) the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer;

(o) the disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual;

(p) subject to the conditions in paragraph 3, the personal data —

(i) is disclosed to a party or a prospective party to a business asset transaction with the organisation;

(ii) is about an employee, customer, director, officer or shareholder of the organisation; and

(iii) relates directly to the part of the organisation or its business assets with which the business asset transaction is concerned;

(q) subject to the conditions in paragraph 4, the disclosure is for a research purpose, including historical or statistical research;

(r) the disclosure is for archival or historical purposes if a reasonable person would not consider the personal data to be too sensitive to the individual to be disclosed at the proposed time; or

(s) subject to the conditions in paragraph 5, the personal data —

(i) was collected by the organisation in accordance with section 17(1); and

(ii) is disclosed by the organisation for purposes consistent with the purpose of that collection.

2. *In the case of disclosure under paragraph 1(c), the organisation shall, as soon as may be practicable, notify the individual whose personal data is disclosed of the disclosure and the purposes of the disclosure.*

3.—(1) *The conditions in this paragraph shall apply to personal data disclosed under paragraph 1(p).*

(2) In the case of disclosure to a prospective party to a business asset transaction —

(a) the personal data must be necessary for the prospective party to determine whether to proceed with the business asset transaction; and

(b) the organisation and prospective party must have entered into an agreement that requires the prospective party to use or disclose the personal data solely for purposes related to the business asset transaction.

(3) If the organisation enters into the business asset transaction, the employees, customers, directors, officers and shareholders whose personal data is disclosed shall be notified that —

(a) the business asset transaction has taken place; and

(b) the personal data about them has been disclosed to the party.

(4) In this paragraph and paragraph 1(p) —

“business asset transaction” means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the business or assets of an organisation other than the personal data to be disclosed under paragraph 1(p);

“party” means another organisation that enters into the business asset transaction with the organisation.

4. *Paragraph 1(q) shall not apply unless —*

(a) the research purpose cannot reasonably be accomplished without the personal data being provided in an individually identifiable form;

(b) it is impracticable for the organisation to seek the consent of the individual for the disclosure;

(c) the personal data will not be used to contact persons to ask them to participate in the research;

(d) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest; and

(e) the organisation to which the personal data is to be disclosed has signed an agreement to comply with —

(i) this Act;

(ii) the policies and procedures relating to the confidentiality of personal data of the organisation that collected the personal data;

(iii) security and confidentiality conditions of the organisation disclosing the personal data;

(iv) a requirement to remove or destroy individual identifiers at the earliest reasonable opportunity; and

(v) a requirement not to use the personal data for any other purpose or to disclose the personal data in individually identifiable form without the express authorisation of the organisation that disclosed the personal data.

5. *For the avoidance of doubt, personal data collected before the appointed day in the circumstances and conditions set out in the Second Schedule shall satisfy paragraph 1(s) notwithstanding that section 17(1) was not in force at the time of the collection.*

Annex 4 – Exceptions from the Access and Correction Requirements

---

FIFTH SCHEDULE

Section 21(2)

EXCEPTIONS FROM ACCESS REQUIREMENT

1. An organisation is not required to provide information under section 21(1) in respect of —

(a) opinion data kept solely for an evaluative purpose;

(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

(c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

(d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

(e) a document related to a prosecution if all proceedings related to the prosecution have not been completed;

(f) personal data which is subject to legal privilege;

(g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

(h) personal data collected, used or disclosed without consent, under paragraph 1(e) of the Second Schedule, paragraph 1(e) of the Third Schedule or paragraph 1(f) of the Fourth Schedule, respectively, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;

(i) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act —

> (i) under a collective agreement under the Industrial Relations Act (Cap. 136) or by agreement between the parties to the mediation or arbitration;
>
> (ii) under any written law; or
>
> (iii) by a court, arbitral institution or mediation centre; or

(j) any request —

> (i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
>
> (ii) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
>
> (iii) for information that does not exist or cannot be found;

(iv) for information that is trivial; or

(v) that is otherwise frivolous or vexatious.

SIXTH SCHEDULE

Section 22(7)

EXCEPTIONS FROM CORRECTION REQUIREMENT

1. Section 22 shall not apply in respect of —

(a) opinion data kept solely for an evaluative purpose;

(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

(c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

(d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or

(e) a document related to a prosecution if all proceedings related to the prosecution have not been completed.

Annex 5 – List of New Silkroutes Group of Companies

List of Entities within NSG

S/N	Legal Name of Entity	Jurisdiction of Business	Contact Person	Contact Details
1			[●]	[●]
2			[●]	[●]
3			[●]	[●]
4			[●]	[●]
5			[●]	[●]
6			[●]	[●]
7			[●]	[●]
8			[●]	[●]
9			[●]	[●]

APPENDIX OF FORMS

Appendix 1 – Personal Data Access/Correction/Withdrawal Request Form

FOR OFFICIAL USE ONLY	
Date of request:	
Name of NSG company:	
Name of requestor:	
Status of requestor:	Employee of NSG / Customer / Other individual (Please select one)
File Reference no.:	

Please select one:

☐ Access your personal data (Section A)

☐ Correct/update your personal data (Section B)

☐ Withdrawal of consent to Collect, Use, and/or Disclose Personal Data (Section C)

Please download the form, complete it, sign it and mail it to The Data Protection Officer at
456, Alexandra Road
#19-02, Fragrance Empire Building
Singapore 119962
Tel : +65 63 770100

PERSONAL PARTICULARS	
Title and Name * Mr / Mrs / Miss / Ms / Dr *Please underline surname*	**NRIC / Passport Number** *[it is mandatory to upload your NRIC or passport here so that we can verify your identity before processing your request]*
Contact Number(s)	**Date of Birth**
Residential Address	
Name of NSG company	**Email Address**
Section A	
Please indicate what personal data you wish to access:	
Section B	
Please indicate what personal data you wish to correct or what personal data has been omitted/missed out in our records:	

Section C
Please describe in as much detail as possible the nature of your request. (To help us respond to your request quickly, please provide as much detail as possible about the consent(s) you wish to revoke. If possible, restrict your request to a particular service or product offering, department, personnel, incident or subject-matter.)
Any other information that may assist us to process your request:

Please note that:

- To process this request, the information in this form may need to be given to NSG affiliates, partners and subsidiaries, as well as third parties (e.g., service providers).
- You will be contacted by NSG if more information is required to process your request.
- Once processed, please allow us a reasonable period of time (within 30 days) to respond to your request. You will be informed of the likely consequences of withdrawing your consent when we respond to you.
- By default, your request will be treated as a full withdrawal of your consent concerning your personal data (i.e., for its collection, use and disclosure). Please indicate clearly in this form if you do not wish to withdraw your consent for us to (i) collect; or (ii) use; or (iii) disclose any of your personal data.
- By completing signing this form, you acknowledge that the information you have provided is true and accurate to the best of your belief.

[Signature: _____]

FOR OFFICIAL USE ONLY	
DENIAL OF CORRECTION REQUEST	
Date/Time of request:	
Requesting Party:	
Nature of relationship with NSG :	
Officer receiving request:	

Reason(s) for not granting correction request:	

Appendix 2 – Non-Disclosure and Security Awareness Undertaking (Third Parties)

IMPORTANT NOTES

1. New Silkroutes Group Limited ("the **Company**") is legally required to comply with the provisions of the *Personal Data Protection Act* (No. 26 of 2012) ("the **Act**"). Failure to comply with the Act may result in penalties being issued against the Company.

2. To ensure compliance with the Company's internal policies in relation to the Act, all third party contractors and/or service providers are required to sign this Undertaking.

3. This Undertaking shall be signed before the commencement of work and/or services for the Company.

A. CONTRACTOR / SERVICE PROVIDER'S DETAILS

1.	**Name of Contractor / Service Provider's Company ("Service Provider"):**	
2.	**Company UEN No:**	
3.	**Contact Number:**	
4.	**Address:**	
5.	**Email Address:**	
6.	**Nature of Work / Service provided to Company ("Purpose"):**	

B. UNDERTAKING

1. Access to Personal data, non-public and sensitive information ("**Confidential Information**") may be required in the performance of the Service Provider's Purpose. "**Personal data**" has been defined in the Act to refer to information about an identified or identifiable individual, where the individual refers to a natural person, whether living or deceased. It covers all forms of personal data, whether in electronic or non-electronic form.

2. The Service Provider shall use the Confidential Information solely for performing the Purpose and for no other purpose whatsoever.

3. Should the Service Provider have access to such Confidential Information, the Service Provider undertakes that it shall keep such Confidential Information in confidence; disclose it only to its employees or authorized representatives on a need-to-know basis and who are under confidentiality restrictions no less restrictive than those set out herein. It shall not under any circumstances, release or disclose such Confidential Information to any third party or third party organisation.

4. The Service Provider shall protect such Confidential Information with at least the same degree of care as it exercises to protect its own confidential information of a similar nature and will use all best endeavours to maintain the confidentiality of the Confidential Information. Notwithstanding the foregoing, the Service Provider shall at all times use reasonable security measures, at least the equal of or better than current industry practices, to ensure the protection of the Confidential Information.

5. The Service Provider shall immediately notify the Company of any suspected or unauthorized disclosure and/or use of Confidential Information or any other breach of security.

6. All Confidential Information will and at all times remain the exclusive property of the Company. The Service Provider shall immediately provide access to, amend, return or destroy any or all Confidential Information upon completion of the Purpose or on request from the Company.

C. CONSEQUENCES OF BREACH OF UNDERTAKING

The Service Provider acknowledges and agrees that:

1. It shall keep the Company fully indemnified against all actions, claims, demands, proceedings, liabilities, losses (whether direct, indirect or consequential), penalties, fines, costs (including legal costs in a full indemnity basis) and expenses of every kind suffered by the Company, its officers or employees, arising out of or in connection with any claim made by a third party, any complaints, investigations or proceedings by any regulatory authority, due to or arising out of any actual or alleged breach or non-performance or non-observance of the Service Provider's obligations under this Undertaking.

2. In the event of any breach or neglect of its obligations under this Undertaking, the Company may exercise its right to refuse its access to the Company's premises and facilities.

3. The restrictions contained in this Undertaking are reasonable in scope and are necessary to protect the Company's legitimate interest in protecting its business.

4. Any breach or threatened breach of its obligations under this Undertaking may result in significant and irreparable damage to the Company that could not be satisfactorily compensated in monetary terms, and for which the remedies at law available to the Company may otherwise be inadequate. Accordingly, in addition to any other remedies to which the Company may be entitled to under law or in equity, the Service Provider acknowledges and agrees that the Company may immediately seek enforcement of this Undertaking by means of injunctive relief, including but not limited to specific performance or an injunction to prevent any unauthorized use, disclosure or breach hereof.

5. Even after the Service Provider ceases its Purpose at the Company, it agrees that the confidential obligations to the Company as set out herein shall continue.

Name of Service Provider: _____

Service Provider's Company Stamp: _____

Name of Representative of Service Provider: _____

Signature of Representative of Service Provider: _____

Date: _____