SANDS
SELKIRK AND SELKIRK - ENGINEERING SOLUTIONS

*Engineering solutions to meet a changing world*

14 Cyclonite Street
The Interchange
Somerset West, 7130
Republic of South Africa

Tel: +27 21 852 5095
Fax: +27 21 852 5070
e-mail: info@selkirkandselkirk.co.za
Web: www.selkirkandselkirk.com

P.O. Box 226
Somerset West, 7130

# SUPPLIER PRIVACY NOTICE

## PROTECTION OF PERSONAL INFORMATION ACT 2013

**PREPARED BY:** **G R SELKIRK**

**DATED: 30 June 2021**

# SUPPLIER PRIVACY NOTICE

Selkirk & Selkirk ("SandS", the "Responsible Party")'s Supplier Privacy Policy applies to all Suppliers who receive and Process Personal Information on behalf of SandS and forms part of the Agreements between such Supplier and SandS which refer to this Policy.

**NOTIFICATION**

a) The Supplier shall immediately inform the Responsible Party in writing of any requests with respect to Personal Information received from the Responsible Party's employees, customers or any Third Party. The Supplier shall respond to such requests in accordance with the Responsible Party's instructions. The Supplier shall cooperate with the Responsible Party if an individual requests access to his or her Personal Information for any reason.

b) Subject to applicable law, the Supplier shall notify the Responsible Party immediately in writing of any subpoena or other Judicial or Administrative Order by a government authority or proceeding seeking access to or disclosure of Personal Information. The Responsible Party shall have the right to defend such action in lieu of and on behalf of the Supplier. The Responsible Party may, if it so chooses, seek a Protective Order. The Supplier shall reasonably cooperate with the Responsible Party in such defence.

c) If the Supplier becomes aware of any Information Security Incident, the Supplier shall, within 24 (twenty four) hours after becoming aware of such Information Security Incident, notify the Responsible Party's local Data Protection Officer in writing of such Information Security Incident, specifying the extent to which Personal Information was or is reasonably believed to have been compromised or disclosed. In addition, the Supplier shall (i) perform a root cause analysis thereon, (ii) investigate such Information Security Incident, (iii) preserve all documents, Personal Information and other Information related to the Information Security Incident and investigation, (iv) provide the Responsible Party with a Remedial Plan, acceptable to the Responsible Party, to address the Information Security Incident and prevent any further incidents, (v) remediate such Information Security Incident in accordance with such approved plan, (vi) conduct a forensic investigation to determine what systems, Personal Information and Information have been affected by such event; and (vii) cooperate with the Responsible Party and, at the Responsible Party's request, any law enforcement or regulatory officials, credit reporting organisations, and credit card associations investigating such Information Security Incident. If the Supplier does not provide to the Responsible Party the results and related reporting associated with its forensic investigation or the Responsible Party determines that such Information is not sufficient, then the Supplier shall allow the Responsible Party and its designees to conduct a forensic investigation of the Information Security Incident. The Supplier shall use commercially reasonable efforts to preserve all evidence relating to the Information Security Incident until the Responsible Party has completed such forensic investigation or confirmed to the Supplier that it waives its right to conduct such an investigation. To the extent that the Supplier is unable to preserve any evidence relating to the Information Security Incident, the Supplier shall create and maintain forensic copies of all such evidence and supporting documentation reasonably necessary for the investigation and prosecution of claims relating to such Information Security Incident.

d) Without limiting the foregoing and notwithstanding anything herein or in the Agreement to the contrary, the Responsible Party shall make the final decision on notifying the Responsible Party's customers, employees, service providers and/or the general public of such Information Security Incident as it relates to the Responsible Party, and the implementation of the remediation plan as it relates to the Responsible Party and the services provided to the Responsible Party under the Agreement. If a notification to any person is required under any Privacy Law, then at the Responsible Party's option notifications to all persons who are affected by the same event (as reasonably determined by the Responsible Party shall be considered legally required.

e) The Supplier will be responsible for the costs and expenses associated with the performance of its obligations in Section II(c) above if the Information Security Incident did not result from the acts or omissions of the Responsible Party or any of its Third Party providers (excluding the Supplier and its designees), and the Supplier shall reimburse the Responsible Party on demand for all Notification Related Costs (as hereinafter defined) incurred by the Responsible Party arising out of or in connection with any such Information Security Incident. The Responsible Party will be responsible for the Supplier's reasonable costs and expenses associated with the performance of its obligations in Section II(c) above, other than the costs and expenses associated with the notification required to be provided to the Responsible Party of the Information Security Incident, if the Information Security Incident resulted from the acts or omissions of the Responsible Party, or any of their Third Party providers (excluding the Supplier). "Notification Related Costs" shall include the Responsible Party's internal and external costs associated with addressing and responding to the Information Security Incident, including but not limited to: (i) preparation and mailing or other transmission of legally required notifications; (ii) preparation and mailing or other transmission of such other communications to such persons as the Responsible Party deems reasonably appropriate; (iii) establishment of a call centre or other communications procedures in response to such Information Security Incident (e.g., frequently asked questions and training); (iv) public relations and other similar crisis management services; (v) legal and accounting fees and expenses associated with the Responsible Party's investigation of and response to such event; and (vi) costs for commercially reasonable credit reporting services that are associated with legally required notifications or are advisable under the circumstances.

**COMPLIANCE WITH PRIVACY AND INFORMATION SECURITY REQUIREMENTS.**

a) The Supplier shall comply with all Privacy Laws as they relate to Personal Information subject to this Policy.

b) The Supplier confirms that no applicable law, or legal requirement, or privacy or Information Security enforcement action, investigation, litigation or claim prohibits the Supplier from (i) fulfilling its obligations under the Agreement with the Responsible Party or (ii) complying with instructions it receives from the Responsible Party concerning Personal Information. In the event a law, or legal requirement, or privacy or Information security enforcement action, investigation, litigation or claim, or any other circumstance, is reasonably likely to adversely affect the Supplier's ability to comply with this Policy, the Supplier shall promptly notify the Responsible Party in writing and the Responsible Party may, in its sole discretion and without penalty of any kind to the Responsible Party, suspend the transfer or disclosure of Personal Information to the Supplier or access to Personal Information by the Supplier, terminate any further Processing of Personal Information by the Supplier, and terminate the Agreement, if the Responsible Party reasonably deems termination necessary to comply with applicable Privacy Laws or to avoid any breach thereof.

c) The Supplier shall enter into any further privacy, Information security, Personal Information transfer or Personal Information Processing Agreement requested by the Responsible Party for purposes of

compliance with applicable Privacy Laws. In case of any conflict between this Policy and any such further Personal Information Privacy or Information Security Agreement, such further Agreement shall prevail with regard to the Processing of Personal Information covered by it.

**PERSONAL INFORMATION SAFEGUARDS**

a) The Supplier shall develop, maintain and implement a comprehensive written Information security programme that complies with applicable Privacy Laws. The Supplier's Information security programme shall include appropriate administrative, technical, physical, organisational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Information; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Information; (iii) protect against any actual or suspected Information Security Incident; (iv) encourage timely internal reporting of reasonably suspected and actual Information Security Incidents; and (v) facilitate appropriate response by the Supplier to Information Security Incidents. Without limiting the generality of the foregoing, the Supplier's Information Security Policies shall provide for (y) regular assessment and re-assessment of the risks to the security of Personal Information and systems used by the Supplier to Process Personal Information, including (1) identification of internal and external threats that could result in an Information Security Incident, (2) assessment of the likelihood and potential damage of such threats, taking into account the sensitivity of such Personal Information and Systems, and (3) assessment of the sufficiency of Policies, Procedures, and Information Systems of the Supplier, and other arrangements in place, to control risks; and (4) protection against such risks.

b) If the Processing by the Supplier or its Personnel involves the transmission of the Personal Information over a network, the Supplier shall implement appropriate measures designed to protect the Personal Information against the specific risks associated with such transmission. The Supplier shall ensure a level of security appropriate to the risks associated with such transmission and the nature of the Personal Information Processed or as otherwise required by Privacy Laws.

c) The Supplier shall exercise the necessary and appropriate supervision over its relevant Personnel to maintain appropriate privacy, confidentiality and security of Personal Information. The Supplier shall provide training, as appropriate, regarding the privacy, confidentiality and Information security requirements set forth in this Policy to relevant Personnel who have access to Personal Information. The Supplier shall only retain contractors that the Supplier reasonably can expect to be suitable and capable of performing the delegated obligations in accordance with the Agreement and this Policy.

d) Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as the Responsible Party's requests, the Supplier shall return to the Responsible Party or its designee, or at the Responsible Party's request, securely destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to the Responsible Party (which decision shall be based solely on the Responsible Party's written statement), each and every original and copy in every media of all Personal Information in the Supplier's possession, custody or control. Promptly following any return or alternate action taken to comply with this paragraph, the Supplier shall provide to the Responsible Party a completed officer's certificate certifying that such return or alternate action occurred. In the event applicable law does not permit the Supplier to comply with the delivery or destruction of the Personal Information, the Supplier warrants that it shall ensure the protection and confidentiality of the Personal Information until such time as delivered or destroyed and that it shall not use or disclose any Personal Information after termination of the Agreement.

**RIGHT TO MONITOR**

a) The Responsible Party shall have the right to monitor the Supplier's compliance with this Policy. During normal business hours, and without prior notice, the Responsible Party or its authorised representatives may inspect the Supplier's facilities, equipment and systems, and any Information or materials in the Supplier's possession, custody or control, relating in any way to the Supplier's

obligations under this Policy. An inspection performed pursuant to this Policy shall not unreasonably interfere with the normal conduct of the Supplier's business. The Supplier shall cooperate fully with any such inspection initiated by the Responsible Party.

b) The Supplier shall deal promptly and appropriately with any inquiries from the Responsible Party relating to the Processing of Personal Information subject to this Policy.

**PURPOSE SPECIFICATION OF PERSONAL INFORMATION**

Any Personal Information supplied by a Data Subject shall only be collected and used by SandS for the purpose for which it was originally intended. In the event that the Personal Information will be used for another purpose, consent from the Data Subject will be obtained prior to the use of such Information.

**ACCURACY OF PERSONAL INFORMATION**

In the event of any changes to the Personal Information of a Supplier, the said Supplier is under an obligation to inform SandS of the said changes within a reasonable period of time.

**CHANGES IN THIS POLICY**

Boron reserves the right to amend, alter and terminate this Policy at any time.

**INFORMATION OFFICER DETAILS**

**Contact Person:** **Gavin Ross Selkirk**

**Tel / Cell:** **083 448 9732**

**E-mail:** **gavin@selkirkandselkirk.co.za**

**Website:** **www.selkirkandselkirk.com**

**Physical /Postal Address:**
**14 Cyclonite Street**
**The Interchange**
**Somerset West**
**7130**

**PO Box 226**
**Somerset West**
**7129**