FRAUD AND SECURITY POLICY

1. **Obligations:**

1.1 This Policy outlines the requirements pertaining to any Security Incident.

1.2 Spliceteq South Communications Ltd (Hereafter in this document referred to as the Company) shall take reasonable measures to prevent fraud and safeguard its own and or Clients property.

1.3 The Company shall ensure that all its Information and or Customer Information and information processing facilities are protected in accordance with the security requirements defined in ISO27001 and Good Industry Practice.

1.4 For new contracts the Parties shall establish a Security Forum within 90 days from the Service Commencement Date and each Party shall provide a Security Representative to attend Security Forum meetings and calls, as outlined in Table 2 of Schedule 5.

1.5 The development and implementation of measures arising from the Security Forum are to be treated as confidential and the Company will exercise appropriate discretion over such information with its Staff.

1.6 The Company shall submit a copy of its security and fraud prevention Policy to its Clients within one (1) Month of the Service Commencement Date so that it may be reviewed by the Clients. The Clients may require changes to be made to the Fraud and Security Policy so that it is in compliance with its own security requirements.

1.7 The Company shall notify the Clients immediately of any Security Incident and confirm in writing to the Client within one (1) Working Day of the Client receiving such notice.

1.8 Clients shall notify the Company of any Security Incident of which it is made aware of as soon as reasonably possible.

1.9 On confirmation of any Security Incident or after notification of any Security Incident, the Company and the Client shall convene a security meeting between the Parties' Security Representatives within two (2) Working Days of such notice to discuss the Security Incident.

1.10 The Company shall complete an investigation within five (5) Working Days of a notification or confirmation of a Security Incident, identify security improvements / corrective measures necessary to resolve it and implement any security improvements or counter measures as soon as reasonably possible once such measures are agreed with the Client.

1.11 Following any confirmed Security Incidents, the Company shall make available to the Client all data, records and information pertaining to the investigation referred to in Paragraph 1.10 above.

1.12 The Company shall procure agreement from all its Staff to the following:

(a) Access by either the Company, Client or authorised bodies to all call data, voicemail and address books of mobile phones supplied by the Company for the purposes of provision of the Services.

(b) Searches of the Company Staff of the person, vehicle and locker, solely for the purposes of the prevention, detection and / or investigation of fraudulent behaviour and or a breach of security.

1.13 The Company shall:

(a) Permit, with prior notice, the Client to enter its premises subject to being escorted by the Company Senior Management, with unrestricted access solely for the purposes of the prevention, detection and or investigation of fraudulent behaviour and or a breach of security;

(b) Always issue, re-issue and transfer Clients equipment with supporting paperwork and in accordance with the Clients applicable transfer processes;

(c) Retain all CPE related paperwork and records as relevant records;

(d) Store all Clients equipment securely and ensure that all issue and return of equipment only takes place in accordance with the Clients issue and return processes;

(e) As far as is practical, ensure that Company Vehicles are void of Clients Equipment each night; and

(f) Initiate perpetual inventory counts on a weekly basis so that the Company is able to account for the location of all Clients Equipment at any time.

1.14 In addition to any audit rights the Clients may have pursuant to Clause 22 of this Policy, the Client may perform two (2) security and fraud audits at the Company Premises or any other location reasonably required by the Client in a Contract Year. The Client may perform an additional security and fraud audit following any confirmed Security Incident.

Paul Parkinson

Paul Parkinson

CEO

21/06/2024