GRASP DATA TRANSLATION SERVICES PROPRIETARY LIMITED

INFORMATION SECURITY POLICY

1 GENERAL

1.1 This Information Security Policy ("**Policy**") together with our terms and conditions as contemplated in our standard services agreement describes the Company's obligations and the Customer's rights in relation to the logical, physical and information security of Customer Data (as defined herein) in respect of the Services provided under the Services Agreement.

1.2 Unless otherwise expressly stated in this Policy or elsewhere in the Services Agreement, the Company's obligations under this Policy shall be carried out at no additional cost to the Customer.

1.3 In the event of any uncertainty that may arise in respect of the application and implementation of this Policy, the Parties shall consult the relationship manager of the Company.

1.4 Unless the context clearly indicates otherwise any obligations described in this Policy are in addition to the obligations described in the Services Agreement, and shall not be interpreted to substitute any other similar obligations described in the Services Agreement.

2 DEFINITIONS

2.1 In this Policy, the following words and terms will, unless otherwise stated or inconsistent with the context in which they appear, bear the following meanings and other words derived from the same origins as such words (that is, cognate words) shall bear corresponding meanings –

2.1.1 "**Company**" means Grasp Data Translation Services Proprietary Limited , registration number 2019/040637/07, a limited liability private company incorporated in accordance with the laws of South Africa;

2.1.2 "**Company IT Systems**" means the information technology and telecommunications infrastructure and systems used by the Company, including computer and telecommunications networks, communication tools and equipment supplied by (or on behalf of) the Company and includes (without limitation) hardware, software, internet access, cloud-based infrastructure, e-mail facilities and

2.1.3 messaging systems (including voicemail facilities), middleware, firmware, peripherals, terminals and components;

2.1.4 "**Customer**" means the customer who has entered into the Services Agreement with the Company;

2.1.5 "**Customer Data**" means any communications and data, including Personal Information (as defined in the Services Agreement) of the Customer —

2.1.5.1 supplied to the Company by or on behalf of the Customer; or

2.1.5.2 stored, used, collected, collated, accessed or processed on behalf of the Company whether through the of the IT Systems or otherwise as part of the Services;

2.1.6 "**DaTS Platform**" means the online DaTs platform which is an integrated system architecture combining a licensed Artificial Intelligence application and a proprietary data enrichment and transformation application, and which developed by the Company used to perform data translation services for the Customer pursuant to the Services Agreement ;

2.1.7 "**Services**" means the services to be provided by the Company to the Customer pursuant to the Services Agreement; and

2.1.8 "**Services Agreement**" means the standard services agreement entered into between the Customer and the Company.

3 INFORMATION SECURITY GOVERNANCE AND COMPLIANCE

3.1 The Company shall comply with all current legal and regulatory requirements relating to information security, as it relates to the Services rendered by the Company to the Customer.

3.2 The Company will be responsible for (i) compliance with the standards, guidelines and procedures set forth in this Policy; (ii) the provisions of the Services Agreement relating to the protecting the confidentiality, integrity, privacy and authenticity of the Customer Data stored on the Company's IT Systems.

3.3 The Company shall, to the extent required by the Services, comply with the international best practice with regards to information security industry standards as it relates to the Services.:

4 SECURITY MEASURES

4.1 The DaTS Platform is fully hosted on the Amazon Web Services ("**AWS**") Infrastructure and accordingly the security procedures applicable to the AWS infrastructure will apply to any of the Customer Data hosted on the DaTS Platform. Should the Customer require further details of such security details, the Company will make it available to the Customer upon request.

4.2 When performing the Services the Company will rely on the AWS Infrastructure and all Customer Data will be fully hosted on the AWS Infrastructure.

The Company will use best endeavours to comply with the following security measures as it relates to the Services:

4.3 **IT Systems security**

4.3.1 The Company will—

4.3.1.1 implement and maintain procedures to provide adequate protection from intrusion of the IT Systems by external or internal sources;

4.3.1.2 comply with such security policies and procedures which may be prescribed or communicated by the Customer from time to time in writing, including—

4.3.1.2.1 taking appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of Customer Data in its possession or under its control;

4.3.1.2.2 identifying all reasonably foreseeable internal and external risks to Customer Data in its possession or control;

4.3.1.2.3 establishing and maintaining appropriate safeguards against the risks identified, and verifying that the safeguards are effectively implemented; and

4.3.1.2.4 ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

4.4 **Anti-virus and malware protection**

4.4.1 The Company will:

4.4.1.1 ensure that it has appropriate anti-virus and malware protection software on all IT Systems used to deliver or support the Services in accordance with good industry practice; and

4.4.1.2 upon detection of any malware incidents or threats on its IT Systems used to deliver the Services, take immediate steps to assess the scope of any damage, arrest the speed of the damage, eradicate the malware and to the extent reasonably possible restore all Customer Data and IT Systems to its original state.

4.5 **Logical, physical and informational security**

4.5.1 The Company will responsible for:

4.5.1.1 establishing and maintaining appropriate safeguards against the unauthorised access, destruction, loss or alteration of Customer Data;

4.5.1.2 managing and administering access to Company-operated devices, systems, networks, software and Customer Data;

4.5.1.3 implementing such supplemental provisions to be consistent with similar security provisions in accordance with good industry practice;

4.5.1.4 following the Customer's instructions and procedures regarding access to the Customer environment for purposes of performing the Services where such access is designated by the Customer;

4.5.1.5 ensuring that Company staff that are involved in the performance of the Services will have the appropriate access clearances for their roles and responsibilities in relation to the Customer environment;

4.5.1.6 developing, maintaining, updating and implementing security procedures including physical access strategies and standards where applicable;

4.5.1.7 the development of an action plan and escalation procedures for any potential or real security breaches, and reporting any potential or real security breaches to the Customer;

4.5.1.8 monitoring the Company IT Systems for authorised access and monitoring, reviewing and responding in a timely and appropriate manner to access breaches and any other relevant anomalies;

4.5.1.9 notifying the Customer in the event of a security breach or unauthorised attempt to access or alter Customer Data;

4.5.1.10 conducting periodic reviews, as appropriate, to validate that individual employee access to the Company IT Systems is appropriate;

4.5.1.11 performing periodic security audits, providing incident investigation support and initiating corrective actions to minimise and prevent security breaches;

4.5.1.12 providing reports on security breaches and access attempts, and retaining documentation of the investigation;

4.5.1.13 establishing procedures, forms and approval for assigning, resetting and disabling user IDs and passwords used for data or system access by authorised users, and e all related administration of user identification (IDs) and passwords;

4.5.1.14 coordinating IT System password changes; and

4.5.1.15 performing backup and recovery procedures in response to security violations that result in lost/damaged information.

5 SECURITY BREACHES

5.1 The Company will:

5.1.1 have in place a formal staff disciplinary process to deal with any Customer Data security breaches, vulnerabilities or risks ("**security risks**");

5.1.2 notify the Customer in writing of any Customer Data security risks as and when the said security risks are identified by the Company or the Company is informed or notified thereof;

5.1.3 conduct a root cause analysis of all security risks, and provide the Customer with all documentation related thereto;

5.1.4 inform and consult the Customer where any of its staff are subject to a change of circumstance that results in such staff becoming a risk to the Services rendered or to Customer Data; and

5.1.5 compile a written report describing all security risks and associated steps taken by the Company to mitigate the security risks and present such report to the Customer upon completion thereof.

6 CHANGES TO THIS POLICY

The Company reserves the right to change this Policy from time to time, and in its sole discretion. The Company may send a notice regarding material changes to this Policy, but the Customer is encouraged to frequently check this Policy for any changes. The Customer's continued use of the AI Converter and/or the Services after any change in this Policy will constitute its acceptance of such changes.

7 HOW TO CONTACT US

Any questions, comments and requests which the Customer may have regarding this Policy are welcomed. If you have any questions, comments and requests about this Policy, please contact the Company at **info@graspdata.co.za** with "*Information Security Policy*" in the subject line.

Last edited on 03 July 2019.

Heading (Corbel Bold 12pts)

Start typing body copy here… (Corbel Regular 11pts)