DATA PLUS – DATA PROTECTION

1 DEFINITIONS

1.1 "**Data Loss Event**" any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach

1.2 "**Data Protection Legislation**" means the Data Protection Act 2018 (as amended, restated or replaced), The General Data Protection Regulations (Regulation (EU) 2016/679, the Privacy and Electronic Communications Regulations 2003 and any related act or regulation in the UK, including statutory modification or re-enactment of it, and "Data", "Data Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Data Processor", and "Process" shall have the meaning specified in the Data Protection Act 2018 (as amended, restated or replaced).

1.3 "**Data Protection Impact Assessment**" means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

1.4 "**Data Subject Access Request"** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data

1.5 "**Data Systems**" means information systems including, but not limited to, net-services, networks, computers, computer systems, communication systems and other information systems; and means of access to such systems including, but not limited to, passwords, tokens, keys, logon scripts or other authentication information.

1.6 "**Protective Measures**" means appropriate technical and organisational measure which may include; pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measure adopted by a Party. The Security measures adopted by Concentra are set out at https://concentra.app.box.com/v/DataPlusSecurity.

2 DATA PROTECTION IMPACT ASSESSMENT

2.1 Concentra shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

2.1.1 a systematic description of the envisaged processing operations and the purpose of the processing;

2.1.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

2.1.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

2.1.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data

3 DATA PROTECTION

3.1 In relation to any Personal Data provided by the Customer to Concentra pursuant to this Contract, the parties agree that the Customer and/or the User is the Data Controller and Concentra is the Data Processor, and Concentra shall:

3.1.1 keep the Personal Data secure and take technical and organisational measures to ensure the continued security of the Personal Data;

3.1.2 notify the Customer without undue delay and as soon as reasonably practicable, if it:

3.1.3 receives a Data Subject Access Request (or purported Data Subject Access Request);

3.1.4 receives a request to rectify, block or erase any Personal Data

3.1.5 receives any other complaint or request relating to the Customer's (or User's) obligations under the Data Protection Legislation;

3.1.6 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

3.1.7 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

3.1.8 becomes aware or a Data Loss Event.

3.1.9 assist the Customer in relation to any subject access request, provided the Customer shall be responsible for Concentra's costs in respect of such assistance, such costs capped at any applicable limit that is imposed by the Data Protection Legislation; and

3.1.10 not Process Personal Data outside the European Economic Area.

3.2 In the event that there is, or it is contemplated that there will be, a transfer of Personal Data outside the European Economic Area to a Sub-Contractor, Concentra shall ensure that,

3.2.1 the Sub-Contractor executes, on behalf of the Customer, the standard contractual clauses set out in Commission Decision 2010/87/EU dated 5th February 2010, or

3.2.2 the Sub-Contractor is certified under the Privacy Shield framework or

3.2.3 there is another specifically approved safeguard for data transfers (as recognised under Data Protection Laws) and/or a European Commission finding of adequacy

3.3 Concentra shall Process Data exclusively in accordance with the written instructions of the Customer as set out in in the Order Form unless otherwise required to do so by Law or otherwise authorised in writing by the Customer.

3.4 Concentra shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

3.5 Concentra shall Process all Data on the basis that it is Confidential Information unless otherwise required by law or by the Customer in writing.

3.6 Where Concentra is Processing Data on behalf of Customer or, its employees in connection with the Services being provided Concentra shall:

3.6.1 designate in writing a primary and alternate IT security program manager to act as Concentra's contact and focal point for its obligations set out in this Appendix; and

3.6.2 develop, implement and maintain a comprehensive information security program with commercially reasonable safeguards to protect Data that is in writing and readily accessible to its employees.

4 DATA LOSS EVENT

4.1 Concentra shall promptly provide all reasonable cooperation and assistance to the Customer in respect of any Data Loss Event; including the provision of all information in Concentra's possession concerning the Data Loss Event.

4.2 Concentra will not, without the prior written consent of the Customer, make any announcement about the Data Loss Event unless required to make a disclosure by applicable law.

4.3 Where the Data Loss Event is the result of a systemic failure of the software / Services the costs of any assistance, provided by Concentra, in the mitigation of the Data Loss Event shall be borne by Concentra. Where the Data Loss Event is the result of error, negligence or malicious act of the Customer or a User, the costs of any assistance, provided by Concentra, in the mitigation of the Data Loss Event shall be borne by Customer and shall be calculated at Concentra's standard consultancy rates as set out in the Agreement.

5 AUDIT

5.1 If requested by Customer during the term of this Contract Concentra shall permit Customer, or a third party chosen by Customer and reasonably agreed to by Concentra, to perform a security assessment ("IT Security Assessment") of Concentra's IT network, compliance with the Data Protection Legislation and associated Services at Customer's sole cost.

5.2 Concentra shall work cooperatively with Customer to determine whether additional or different security measures are required to protect the Data Processed or proposed to be Processed on behalf of Customer.

5.3 Concentra and Customer shall mutually agree upon the industry standard tools and manual techniques to be used in conducting this IT Security Assessment. Results of an IT Security Assessment shall be treated as Concentra's Confidential Information unless disclosure is otherwise required by Law.

5.4 If Customer reasonably determines that any portion of the IT Security Assessment must be performed at Concentra's Facilities, then such on-site IT Security Assessment will be performed

5.4.1 at Customer's expense for travel, per diem and any other cost incurred by Customer,

5.4.2 during Concentra's or its agents normal business hours

5.4.3 on a date and time mutually agreeable to Concentra and Customer and

5.4.4 pursuant to any other restrictions and/or limitations mutually agreed to by Customer and Concentra in writing.

6 TECHNICAL AND ORGANISATIONAL SECURITY

6.1 Concentra shall maintain or establish commercially reasonable physical, technical and administrative safeguards that provide for the following:

6.1.1 protection of business facilities, paper files, servers, computing equipment, including all mobile devices and other equipment with information storage capability, and backup systems containing the Data;

6.1.2 network, application (including databases) and platform security;

6.1.3 secure transmission and storage of Data (whether by Encryption or other equally protective measures);

6.1.4 Authentication and access control mechanisms;

6.1.5 personnel security; and

6.1.6 audit access to Data and periodically review the audit logs for both valid and invalid access.

6.2 Concentra shall:

6.2.1 provide training and ongoing awareness to Concentra's employees and temporary workers of their obligations in regard to Customer Confidential Data and in particular regarding compliance with physical, technical, and administrative IT security safeguards and compliance with this Appendix ("**IT Security Training**");

6.2.2 require Concentra's subcontractors who provide services in support of Customer and receive Customer Confidential Data in connection therewith to administer IT Security Training to any of its employees and contingent/ temporary workers who provide Services in support of Customer;

6.2.3 regularly test and monitor the effectiveness of its security practices and procedures relating to its compliance with Concentra's information security program and take commercially reasonable measures to adjust its information security program in light of the results of such testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Concentra knows or reasonably should know may have a material effect on its information security program;

6.2.4 impose all requirements related to confidentiality and the handling of Data imposed on Concentra under the Contract and this Appendix on all subcontractors and third parties who have access to or Process Data and perform reasonable ongoing reviews of such subcontractors' capabilities to comply with such requirements

6.3 Concentra shall:

6.3.1 prevent terminated employees from accessing records or systems containing Data;

6.3.2 impose disciplinary measures for violations of Concentra's information security program;

6.3.3 meet or exceed the Minimum IT Security Requirements set forth in this Appendix.

6.4 In the performance of the Services and whilst Processing Data on behalf of Customer, Customer employees, or Customer clients in connection with Services being provided to Customer, Concentra shall not:

6.4.1 bypass its contractual obligations under the Contract and this Schedule;

6.4.2 store Data on any portable computing device including, but not limited to, personal data assistant (PDA), cell phone, Smartphone, laptop (each a "**Portable Computing Device**"), unless Data stored on such Portable Computing Devices is Encrypted;

6.4.3 store Data on any removable media, such as compact disc, flash drive, tape (each a "**Removable Media**"), unless Data stored on such Removable Media is Encrypted;

6.4.4 sell, rent, transfer, distribute or otherwise disclose Data to any third party (including subcontractors and outsourcers) unless required by law enforcement or government bodies (e.g. search warrant, subpoena, court order, etc.) or as otherwise authorised in writing by Customer.

6.5 In the event that a legal body or government agency requests access to the Data Concentra will, unless restricted from doing so by operation of law or applicable regulation, take reasonable steps to provide 48 hours' notice to the Customer of any such request before any such information is disclosed.

7 DATA RETENTION

7.1 On the written instruction of the Customer, or on the termination or expiration of the Contract or the relevant Work Order ("Deletion Notice"), Concentra shall dispose of all Data, including, without limitation, any and all copies and derivatives thereof, in a manner consistent with this Appendix and no later than 30 calendar days (or such other time period as required by Customer) following such Deletion Notice.

7.2 Upon Customer's written request, Concentra shall present Customer with written confirmation of such completion of Data return and/or disposal.