DATA PLUS – SECURITY SCHEDULE

1 INTRODUCTION

1.1 The Customer acknowledges that DataPlus is a Software as a Service ("SaaS") product that is hosted by Concentra's Subcontractor. The product is multi-tenanted where each client shares the same software and physical architecture but where individual client data or tenant data is logically segregated and independently encrypted using unique keys.

1.2 The Customer further acknowledges that whilst Concentra takes all reasonable steps to secure and protect the Customer Data, as detailed in this Security Appendix, it is not possible to guarantee such security.

1.3 Where there is mutually agreed divergence between the terms of this Security Schedule and the standard security requirements of the Customer the Parties will remediate, where reasonably possible, any such divergence between the two. This clause 1.3 shall in no way guarantee that this Security Schedule shall be amended to conform to the Customers standard security requirements.

2 DEFINITIONS

2.1 **Encrypted or Encryption**: the process by which Data is converted into private code to ensure secure transmission or storage.

2.2 Security Breach:

2.2.1 An unauthorized actual physical or logical trespass on a facility, computing systems and/or Data Systems;

2.2.2 Intrusion/hacking of hosted Customer Data, loss/theft of a computer (notebook, desktop, other mobile device, hard drive, or any information storage device); and/or

2.2.3 The unauthorized alteration or destruction of Data; and/or systems

2.3 **Concentra's Facilities**: those real properties on which Concentra or its agents, employees or subcontractors Processes Data on behalf of the Customer.

3 VULNERABILITY SCANNING & IT SECURITY AUDITS

3.1 Vulnerability Scanning. During the Initial Term and any Extended Term of the Contract Concentra agrees the Customer may perform vulnerability assessments using industry standard tools and manual techniques to assess the security of internet facing solution(s) provided by Concentra and used in support of Customer employees, Customer suppliers, and/or Customer customers in connection with Services being provided to Customer ("Vulnerability Scanning"). As to Vulnerability Scanning which Customer may conduct, the following shall apply:

3.1.1 Vulnerability Scanning results shall be treated as Concentra Confidential Information unless disclosure is otherwise required by Applicable Law;

3.1.2 Vulnerability Scanning will be performed by authorised cyber security professional(s) agreed between the parties in advance of the Vulnerability Scanning taking place;

3.1.3 Authorised Customer cyber security professional(s) may work with Concentra to manually validate findings on production and test systems in order to help reduce false positives. Authorised Customer cyber security professional(s) may also contact Concentra's designated IT security program manager should any additional information or work be required as part of Vulnerability Scanning;

3.1.4 Concentra's Information Security Officer will be notified by Customer of any major security vulnerabilities and such vulnerability notification shall be treated as Confidential Information;

3.2 Routine IT Security Compliance Audit. Upon at least thirty (30) calendar days advanced written notice from Customer, Concentra shall grant Customer (or a 3rd Party on Customer's behalf and reasonably approved by Concentra) permission to perform a routine, non-invasive audit of Concentra's environment in order to ensure compliance with this Schedule, the Contract, and laws, regulations, directives, ordinances, and industry standards relative to Concentra's Processing of Data ("Routine IT Security Compliance Audit"). Such Routine IT Security Compliance Audit will be performed subject to the limitations set forth below and at Customer's expense for travel and per diem incurred by Customer and will only be performed after written confirmation is received from the Concentra.

3.3 IT Security Audit – Notification of Security Breach. In the event of a Security Breach Customer may conduct follow up IT Security Breach Audits ("Follow Up IT Security Breach Audit(s)"), as required, in order to confirm Concentra's corrective actions to any findings addressed in the respective Remediation Plan (defined below). An IT Security Breach Audit (whether Initial or Follow Up) will be performed (1) during Concentra's normal business hours, (2) on a date and time mutually agreeable to Concentra and Customer (3) at Customer's expense for travel and per diem incurred by Customer. Concentra shall document Concentra's responsive actions taken in connection with a Security Breach in accordance with all Applicable Laws. Customer reserves the right to be a participant in, and Concentra shall cooperate with such participation in, any Security Breach investigations involving Data, including Customer's review of forensic data relating to the Security Breach.

3.4 Remediation Plan. Any findings during an IT Security Audit will be addressed in a mutually agreed upon remediation plan and Concentra shall comply with, and complete, such remediation plan within a mutually agreeable timeframe set forth therein ("Remediation Plan").

4 NOTIFICATION

4.1 Notification of Inquiry. Except where expressly prohibited by law or where expressly waived in writing by Customer, Concentra shall notify Customer of any subpoena, judicial, administrative or arbitral order or any demand or information request from an executive or administrative agency, other governmental or authority, or Customer employee that it receives (each, for purposes of this Appendix, an "Inquiry") which impacts Concentra's use or security practices affecting Data Processed on behalf of Customer. Such notification should include any details of such subpoena, order, demand or request as known to the Concentra ("Notification"). Concentra shall use commercially reasonable efforts to provide Customer with Notification within 48 hours after Concentra becomes aware of an Inquiry.

4.2 Notification of Security Breach. In the event that Concentra experiences a Security Breach affecting Data Processed on behalf of Customer, Concentra shall use commercially reasonable efforts to provide Customer with Notification within 24 hours after Concentra becomes aware of the Security Breach. In the event of any Security Breach, Customer shall have sole control over the timing, content and method of notification to its clients and third parties.

4.3 Assistance. Upon Customer's request and at Customer's expense, Concentra shall promptly provide Customer with such information and assistance regarding Concentra's Processing of Personal Data, if applicable, as is required by any court of competent jurisdiction or national regulatory authority, or as is required to timely respond to or otherwise address any Inquiry, access request, complaint, enforcement notice, claim or similar action made by any or all subjects of Data.

4.4 Reimbursement of Costs. If a Security Breach or unauthorised access results from any act or omission of Concentra or any Concentra Personnel, Concentra shall promptly reimburse Customer for all costs and expenses Customer may incur in providing any notification of such security breach or unauthorised access or otherwise complying with applicable legal requirements triggered by such Security Breach subject always to the limitations of liability as set out in this Contract.

5 NETWORK SECURITY

5.1 Concentra shall be solely responsible for ensuring that Concentra employees are not security risks, and upon Customer's request, Concentra will provide Customer with any information reasonably necessary for Customer to evaluate security issues relating to any Concentra employee who is directly involved in providing the Services.

5.2 Each party will be solely responsible for ensuring their security procedures and policies are sufficient to ensure that (a) such party's use of its network is secure and is used only for authorised purposes, and (b) such party's business records and Data are protected against improper access, use, loss alteration or destruction.

5.3 Upon written request, Concentra shall provide Customer with a network diagram that outlines Concentra's I/T network involved in storing or enabling access to Data.

6 USE OF CRYPTOGRAPHY

6.1 Data transmitted over any unsecure network or wirelessly is Encrypted using TLS v1.2 or better.

6.2 Data is Encrypted at rest using AES-256 (GCM)

7 DISASTER RECOVERY

7.1 Concentra shall maintain a disaster recovery plan for restoring its current and off-site Data files Processed pursuant to the Contract.

7.2 Concentra will be responsible for backup and preservation of any Data Processed on behalf of Customer. All backup copies of Data shall be treated as Confidential Data and are Encrypted.

7.3 Concentra will maintain a business continuity plan for restoring its critical business functions.

7.4 Upon request from Customer, Concentra must show evidence that the disaster recovery plan relating to the Services is tested and exercised on a regular basis to ensure that Customer or Customer client Data is protected from disaster.

8 MINIMUM IT SECURITY REQUIREMENTS

8.1 Concentra shall use commercially reasonable efforts to either meet or exceed the requirements as set out below. For the avoidance of doubt, the requirements shall apply only to those Concentra systems where Customer Data is processed.

8.2 Administrative privileges will only be used to set up the Customer Tenant and to set up the Customer Administrator. Administrative privileges will not be used for any other purpose unless agreed to in writing by both Concentra and Customer.

8.3 The Customer Administrator is responsible for:

8.3.1 Setting up all other Customer Users

8.3.2 Ensuring Users are granted appropriate permission to access, use and transform Customer Data.

8.3.3 Ensuring access privileges are removed from those Users who no longer have the rights associated with access, use and transformation of Customer Data (e.g as a consequence of leaving the Customers employment, moving department etc)

8.3.4 Managing and assigning users from Concentra who may be required to assist on specific projects. Such controlled Concentra access is solely the responsibility of the Customer Administrator to administer.

8.4 Concentra will ensure that it takes reasonable steps to protect the following Confidential Data:

8.4.1 Information related to the physical location of where the Data is stored (whether Data is stored at an Customer site or at a Concentra's site);

8.4.2 Configuration of systems which store Data; and

8.4.3 Security and management practices in place to protect Data from unauthorised disclosure.

8.5 Concentra maintains processes followed by Concentra employees to verify system configuration, detect security vulnerabilities, validate system integrity, and promptly respond to any deficiencies detected. These processes are used to log, detect, report, and resolve any events which may compromise the security of the system.

8.6 Concentra logs:

8.6.1 Details for the installation and removal of application programs or operating system.

8.6.2 Denied access attempts to critical files.

8.6.3 All authentication transactions.

8.7 Logical Access Control. Concentra ensures through its provision of the Software that systems holding Customer or Customer client Data is authenticated through controls as documented herein.

8.8 Concentra's ensures that the following are adhered to where Data is located at Concentra's Facilities or at the designated hosting location:

8.8.1 Access to areas where Customer Data is stored is controlled and restricted to authorised persons only and authentication controls, e.g. access control card are used to authorise and validate the access; an audit trail of all access, including times, is securely maintained;

8.8.2 Date and time of entry and departure of visitors is recorded, and all visitors are escorted and supervised; they are only granted access for specific, authorised purposes and are issued with instructions on the security requirements of the area and on emergency procedures;

8.8.3 Access to areas where Data is Processed has cages or secured doors, and is controlled and restricted to authorised persons only;

8.8.4 Authentication controls, e.g. access control card, are used to authorise and validate all access and an audit trail of all access is securely maintained;

8.8.5 Systems are protected against interference with configuration or continued operation; and

8.8.6 Video camera and recording devices monitor all physical traffic in/out of any egress point of any data centre were Customer data is stored. Recordings are stored for a minimum of 15 days.

8.8.7 Video camera surveillance does not capture keyboard and/or console actions and information.

8.8.8 Hardcopy materials are destroyed when no longer needed for business or legal purposes in a manner which ensures that Data cannot be reconstructed.

8.9 Backup and Recovery

8.9.1 Concentra maintains a backup cycle of daily backups that are cycled through every 30 days.

8.9.2 Backup media is Encrypted.

8.10 Anti-Virus Configuration

8.10.1 Live environments on which the Software operates have current anti-virus software configured. All systems that store Data have reasonable up-to-date versions of system security agent software which include malware protection with current virus definitions.

8.11 MALICIOUS USE OF SOFTWARE OR HARDWARE

8.11.1 Concentra and or its hosting partner may use diagnostic tools to support applications, computing systems, and networks. Diagnostic tools may only be used by personnel whose job function requires usage and usage must be limited to those applications, computing systems, and networks within the person's scope. Tools that might impact the performance of the services provided pursuant to the Contract through degradation of availability or performance must receive approval from Customer before they are used.

8.11.2 Data gathered as a result of sniffing any network traffic is protected against unauthorised disclosure, alteration, and destruction. Such Data is only stored if necessary and must be immediately and securely disposed of when no longer needed.

8.12 PROTECTION OF PASSWORDS

8.12.1 This section covers the maintenance of passwords in so far as they are relevant to the Services and Software being provided. Concentra ensures its services/software complies with the following:

8.12.2 Passwords are stored securely not in plain text.

8.12.3 Users are able to change their own passwords.

8.12.4 Each User is accountable and responsible for any action taken with that User's User ID or Username and password. Users are prevented from running concurrent sessions with the same user identity.

8.12.5 The display and printing of passwords is masked, suppressed, or otherwise obscured such that unauthorised parties will not be able to observe or subsequently recover them.

8.12.6 Passwords are not logged or captured as they are being entered.

8.12.7 Passwords are encrypted when transmitted across any network.

8.12.8 User passwords are not stored or used in clear text for the purpose of automating a login sequence

8.12.9 Password change processes do not circumvent password security controls.

8.12.10 Identity Verification and Secure Delivery measures are required for all password resets performed.

8.12.11 Password Complexity Requirements. Password complexity is enforced by the Software and requires not less than 3 out of 4 character classes and must have character class choices such as upper case letters, lower case letters, numeric digits, or special characters (such as $, &, #, @, etc).

8.12.12 Password Length Requirements. Password length is enforced by the Software and is not less than eight (8) characters.

8.12.13 Password Lockout. The Software will lockout a User after a period of inactivity of 1 hour.

8.12.14 Password Expiration. Passwords changes are not enforced by the Software and if required must be manually updated by a process operated by the Customer.

8.13 NETWORK SECURITY

8.13.1 Concentra utilises intrusion detection and prevention system (IDS/IPS) technology as part of the supporting infrastructure. The IDS/IPS is there to protect the multi-tenanted environment and is not intended to provide dedicated protection for individual Customers.

8.14 SECURITY EVENT LOGGING

8.14.1 Concentra collates auditable time stamped logs of the following devices and systems. These logs are not available to Customers as a result of potential Confidentiality conflicts with other customers using the Service, however appropriate summary information may be made available in the event of a Security Breach. The following systems may be monitored:

8.14.2 Network and application firewall devices Network devices that implement Network Address Translation (NAT) and proxy servers;

8.14.3 All server platforms;

8.14.4 Database management systems;

8.14.5 Application middleware; and

8.14.6 Physical Access Control Systems (badge readers, etc.).

8.14.7 Intrusion Detection Systems

8.14.8 Web Server Applications

8.14.9 Hosted Cloud Applications

8.14.10 Log entries must contain the date and time at which the event occurred.

8.14.11 Log Access Control. Logs are labelled as “Confidential” and are protected from unauthorised disclosure, alteration, and destruction.

8.15 ORGANISATIONAL SECURITY

8.15.1 Concentra is ISO 27001 certified and maintains a formal Information Security Management System as part of the requirements of the standard.

8.15.2 Risk Management – Concentra maintains a Risk management policy to identify and evaluate risks associated with adoption of new technologies and changes to existing technologies. Senior management shall review identified risks.

8.15.3 IT Security Policies – Concentra maintains a comprehensive set of information security policies aligned to the requirements of ISO 27001.