ORGVUE – SECURITY PROVISIONS

1 INTRODUCTION

1.1 OrgVue is a Software as a Service product within Concentra's proprietary modules of Software applications. These Security Provisions apply only to the provision of the OrgVue product when ordered by the Client in accordance with Concentra's document entitled the "**Terms and Conditions**". References in these Security Provisions to the "Software" shall therefore be to the software within the OrgVue product only.

1.2 The Client acknowledges that the Software together with the Client Data is hosted by the Subcontractor in the European Economic Area ("**EEA**"). Concentra will not transfer the Client Data outside of the EEA without the Client's prior written approval.

1.3 The Software is multi-tenanted where each Client shares the same software and physical architecture but where the Client Data and Usage Data is logically segregated and independently Encrypted using unique keys.

1.4 The Client acknowledges and agrees that whilst Concentra takes all reasonable steps to secure and protect the Client Data, as detailed in these Security Provisions, it is not possible to guarantee its security.

2 DEFINITIONS

Unless specified otherwise below, capitalised words and expressions contained with this document have the same meaning as set out in the Terms and Conditions:

2.1 **API:** ("Application Programing Interface") is defined as a set of methods for providing programmatic access to functionality offered by Concentra.

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

2.3 **Network Connection**: a connectivity method to the Client's network which is agreed with the Client and is compliant with these Security Provisions.

2.4 **Portal**: any User access method for configuration, management, or use of the Software.

2.5 **Security Breach**:

2.5.1 An unauthorised actual, physical or logical trespass on a facility and/or computing systems that contain the Client Data;

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

2.5.3 The unauthorised alteration or destruction of Client Data and/or systems that contain it.

2.6 **Concentra's Facilities**: those real properties on which Concentra or its agents, employees or subcontractors processes Client Data.

3 VULNERABILITY SCANNING & IT SECURITY AUDITS

3.1 Vulnerability Scanning. During the Term , Concentra agrees the Client may perform vulnerability assessments using industry standard tools and manual techniques to assess the security of internet facing solution(s) provided by Concentra in connection with the Services provided to the Client ("**Vulnerability Scanning**"). As to Vulnerability Scanning which Client may conduct, the following shall apply:

3.1.1 Vulnerability Scanning must be limited to the Software and not the underlying Amazon Web Services platform services or infrastructure.

3.1.2 Vulnerability Scanning results or other related information shall be treated as Usage Data and Concentra Confidential Information unless disclosure is otherwise required by Applicable Law;

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

3.1.4 authorised Client 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 Client 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;

3.1.5 Concentra's IT security program manager will be notified by Client of any major security vulnerabilities;

3.1.6 Concentra will further ensure that the Client may perform Vulnerability Scanning on its hosting partner. In the event that such a test is required the Client agrees to give at least 14 days prior notice of such a test and Concentra will ensure it has written authorisation from such 3rd party allowing Client to conduct Vulnerability Scanning. No such test shall be permitted unless and until such written permission is received;

3.2 Routine IT Security Compliance Audit. Upon at least twenty (20) Working Days advanced written notice from the Client, Concentra shall grant to the Client (or a 3rd party on Client's behalf and reasonably approved by Concentra) permission to perform a remote (i.e. not on-site or in-person), routine, non-invasive assessment of Concentra's technology environment in order to ensure compliance with these Security Provisions and the Terms and Conditions, ("**Routine IT Security Compliance Assessment**"). Such Routine IT Security Compliance Assessment will be performed subject to the limitations set forth below and at Client's expense and will only be performed after written confirmation is received from the Concentra.

3.3 IT Security Assessment – In the event of a Security Breach Client may conduct an IT Security Breach Assessment ("**IT Security Breach Assessment**"), 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 Assessment will be performed (1) during Concentra's normal business hours, (2) on a date and time mutually agreeable to Concentra and Client (3) at Client's expense. Concentra shall document its responsive actions taken in connection with a Security Breach. Client reserves the right to be a participant in, and Concentra shall cooperate with such participation in, any Security Breach investigations involving Client Data, including Client's review of forensic data relating to the Security Breach.

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

3.5 The Client shall be responsible for any costs arising from Concentra's provision of assistance to the Client in respect of these Security Provisions. Such assistance shall not include the implementation of a Remediation Plan.

4 NOTIFICATION

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

5 NETWORK SECURITY

5.1 Concentra shall be solely responsible for ensuring that Concentra staff are not security risks by ensuring that:

5.1.1 it provides training and ongoing awareness to its staff concerning compliance with these Security Provisions;

5.1.2 ensures that its staff comply with these Security Provisions;

5.1.3 regularly tests and monitors its staff's compliance with these Security Provisions;

5.1.4 any terminated staff member no longer has access to Concentra's IT systems and Client Data upon them no longer being a member of staff of Concentra; and

5.1.5 it imposes any disciplinary measures against staff who violate these Security Provisions.

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 IT 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 Concentra shall test and monitor the effectiveness of these Security Provisions on regular basis.

5.4 Upon written request, Concentra shall provide Client with a network diagram that outlines Concentra's IT network involved in storing or enabling access to data.

6 USE OF CRYPTOGRAPHY

6.1 Data transmitted over any network 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 Client Data files processed pursuant to the Agreement.

7.2 Concentra will be responsible for backup and preservation of any Client Data. All backup copies of Client Data shall be treated as Client Confidential Information and will retain encrypted state via AES-256 (GCM). Concentra will maintain a business continuity plan for restoring its critical business functions.

7.3 Upon request from the Client, Concentra must show evidence that the disaster recovery plan relating to the Services is tested and exercised on a regular basis.

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 IT systems where Client Data is processed.

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

8.3 The Client Administrator is responsible for all User Management including:

8.3.1 setting up all Users' access to the Tenant;

8.3.2 ensuring Users are granted appropriate permission to access and use of the Software and Client Data;

8.3.3 ensuring access privileges are removed from those Users who no longer have the rights (e.g. as a consequence of leaving the Client's employment, engagement or moving department etc.); and

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 Client Administrator to administer.

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

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

8.4.2 configuration of IT systems which store Client Data; and

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

8.5 Concentra maintains processes followed by Concentra employees to verify IT 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 IT system.

8.6 Logical Access Control. Concentra ensures through its provision of the Software that IT systems holding Client or Client Data is authenticated through password control as documented herein.

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

8.7.1 access to areas where Client 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;

8.7.2 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;

8.7.3 access to physical areas where Client Data is processed has cages or secured doors, and is controlled and restricted to authorised persons only;

8.7.4 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;

8.7.5 IT systems are protected against interference with configuration or continued operation; and

8.7.6 video camera and recording devices monitor all physical traffic in/out of any egress point of any physical data centre where Client Data is stored. Recordings are stored for a minimum of 10 Working Days.

8.7.7 video camera surveillance does not capture keyboard and/or console actions and information.

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

8.8 Backup and Recovery

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

8.9 Anti-Virus Configuration

8.9.1 Live environments on which the Software operates have current anti-virus software configured for automatic updates at least once per day. All IT systems that store the Client Data have reasonable up-to-date versions of system security agent software which include malware protection with current virus definitions.

8.10 MALICIOUS USE OF SOFTWARE OR HARDWARE

8.10.1 Concentra and or its Subcontractor 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 Agreement through degradation of availability or performance must receive approval from Client before they are used.

8.11 PROTECTION OF PASSWORDS

8.11.1 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:

8.11.2 passwords are securely hashed and only these hashes are stored;

8.11.3 users are able to change their own passwords;

8.11.4 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;

8.11.5 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.

8.11.6 passwords are not logged or captured as they are being entered;

8.11.7 passwords are Encrypted when transmitted across any network;

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

8.11.9 password change processes do not circumvent password security controls; and

8.11.10 identity verification and secure delivery measures are required for all password resets performed.

8.11.11 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).

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

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

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

8.12 NETWORK SECURITY

8.12.1 Concentra provides an intrusion detection and prevention system (IDS/IPS) as part of the managed hosting service. The IDS/IPS is there to protect the multi-tenanted environment and is not intended to provide dedicated protection for individual Clients.

8.13 PATCHING REQUIREMENTS

8.13.1 Concentra maintains security software so as to remain within one generation of the then current maintenance releases and remain on a supported release. This shall include, but not be limited to, the obligation to promptly implement any security-related enhancement or fix made available by Concentra of such security software.

8.13.2 Concentra maintains detailed procedures for ensuring the stability and security of its IT systems, including regular patching of workstations and servers. Out-of-band patching to address immediate threats is conducted on an expedited basis using all available resources and according to a scheduled based on the severity of the threat.

8.13.3 Patch Management. Prior to defining and implementing a critical patch, sufficient analysis and/or testing is be performed by Concentra to establish that: (a) the patch correctly fixes the vulnerabilities; and (b) the patch does not inadvertently introduce new vulnerabilities.

8.13.4 Concentra will perform reasonable and appropriate analysis and/or testing to establish that security patches do not compromise access to the Software or introduce defects into it.

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 the Client as a result of potential confidentiality conflicts with other clients using the Software, 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;

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; and

8.14.12 log entries are retained for a period of 12 months unless otherwise required by law.

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 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.