SUPPLYVUE – SECURITY PROVISIONS

SupplyVue

1 INTRODUCTION

1.1 SupplyVue is a Software as a Service product and these Security Provisions apply only to the provision of the SupplyVue product when ordered by the Client in accordance with SupplyVue's End User Subscription Agreement (EUSA). References in these Security Provisions to the "Software" shall therefore be to the software within the SupplyVue product only.

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

1.3 The Client acknowledges and agrees that whilst SupplyVue 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 Programming Interface") is defined as a set of methods for providing programmatic access to functionality offered by SupplyVue.

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

3 VULNERABILITY SCANNING & IT SECURITY AUDITS

3.1 Vulnerability Scanning. During the Term , SupplyVue 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 SupplyVue 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 platform services. or infrastructure.

3.1.2 Vulnerability Scanning results or other related information shall be treated as Usage Data and SupplyVue 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 SupplyVue 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 SupplyVue's designated IT security program manager should any additional information or work be required as part of Vulnerability Scanning;

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

3.1.6 In the event that such testing is required, the Client agrees to give at least 14 days prior notice to SupplyVue.. 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, SupplyVue shall grant to the Client (or a 3rd party on Client's behalf and reasonably approved by SupplyVue) permission to perform a remote (i.e. not on-site or in-person), routine, non-invasive assessment of SupplyVue's technology environment in order to ensure compliance with these Security Provisions, ("**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 SupplyVue.

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 SupplyVue's corrective actions to any findings addressed in the respective Remediation Plan (defined below). An IT Security Breach Assessment will be performed (1) during SupplyVue's normal business hours, (2) on a date and time mutually agreeable to SupplyVue and Client (3) at Client's expense. SupplyVue shall document its responsive actions taken in connection with a Security Breach. Client reserves the right to be a participant in, and SupplyVue 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 SupplyVue 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 SupplyVue'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 SupplyVue experiences a Security Breach affecting Client Data, SupplyVue shall

use commercially reasonable efforts to notify the Client within 24 hours after SupplyVue 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 SupplyVue shall be solely responsible for ensuring that SupplyVue 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 have access to SupplyVue's IT systems and Client Data upon them no longer being a member of staff of SupplyVue; and

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

5.2 Upon the Client's request, SupplyVue will provide the Client with any information reasonably necessary for Client to evaluate security issues relating to any SupplyVue staff who are directly involved in providing the Services.

5.3 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.

5.4 SupplyVue shall test and monitor the effectiveness of these Security Provisions on regular basis.

5.5 Upon written request, SupplyVue shall provide Client with a network diagram that outlines SupplyVue'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 higher.

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

7 DISASTER RECOVERY

7.1 SupplyVue shall maintain a disaster recovery plan for restoring its current and off-site Client Data files processed pursuant to the Agreement.

7.2 SupplyVue 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). SupplyVue will maintain a business continuity plan for restoring its critical business functions.

7.3 Upon request from the Client, SupplyVue 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 SupplyVue 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 SupplyVue IT systems where Client Data is processed.

8.2 The Client is responsible for communicating all User Management requirements to SupplyVue in writing. SupplyVue Administrators will then be responsible for ensuring the accurate execution of those requirements, including:

8.2.1 setting up all Users' access to the Tenant;

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

8.2.3 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.).

8.3 SupplyVue will ensure that it takes reasonable steps to protect the following Confidential Information:

8.3.1 information related to the physical location of where the Client Data is stored (whether Client Data is stored at Client site or at SupplyVue's site);

8.3.2 configuration of IT systems which store Client Data; and

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

8.4 SupplyVue maintains processes followed by SupplyVue 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.

8.5 SupplyVue logs:

8.5.1 details for the installation and removal of application programs or operating system;

8.5.2 denied access attempts to critical files; and

8.5.3 all authentication transactions.

8.6 Logical Access Control. SupplyVue 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 Client Data is stored in Microsoft Azure and SupplyVue ensures

8.7.1 All users access the Client Data through secure communication channels as described above;

8.7.2 If Client Data is processed on individual machines these machines are password protected and encrypt Data at rest and in transit, VPN is used on untrusted networks, and access to the Azure environment is controlled by Microsoft Entra ID with audit trail;

8.7.3 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; and

8.7.4 IT systems are protected against interference with configuration or continued operation.

8.8 Backup and Recovery

8.8.1 SupplyVue maintains a backup cycle of daily backups that are cycled through every 10 Working 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 SupplyVue 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.

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

8.11 ACCESS CONTROL

8.11.1 User authentication and authorisation is achieved through Microsoft Entra ID guest users integration, on the client's written instruction

8.11.2 Sign-in and session controls are provided by Microsoft Entra ID.

8.11.3 each User is accountable and responsible for any action taken with that User's User ID or Username.

8.12 NETWORK SECURITY

8.12.1 SupplyVue 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 SupplyVue 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 SupplyVue of such security software.

8.13.2 SupplyVue 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 SupplyVue to establish that: (a) the patch correctly fixes the vulnerabilities; and (b) the patch does not inadvertently introduce new vulnerabilities.

8.13.4 SupplyVue 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 SupplyVue 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 intrusion detection systems;

8.14.7 web server applications;

8.14.8 hosted cloud applications.

8.14.9 log entries must contain the date and time at which the event occurred;

8.14.10 log Access Control. Logs are labelled as "Confidential" and are protected from unauthorised disclosure, alteration, and destruction; and

8.14.11 log entries are retained for a period 180 days unless otherwise required by law. 8.15

ORGANISATIONAL SECURITY

8.15.1 SupplyVue is certified to ISO/IEC 27001:2022 and maintains a formal Information Security Management System as part of the requirements of the standard.

8.15.2 Risk Management – SupplyVue 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 – SupplyVue maintains a comprehensive set of information security policies aligned to the requirements of ISO 27001.