SupplyVue
By CONCENTRA

SECURITY

This document is intended to provide information and assurance on the key information security controls for SupplyVue

As an ISO 27001:2013 and CSA STAR certified organisation, Concentra is fully committed to information security for SupplyVue by providing resource and financial commitments to the establishment, adoption and continual improvement of our security controls and procedures. Security is built-in to the development lifecycle of SupplyVue with risks being continually assessed as part of development and quality control processes. SupplyVue is delivered as Software as a Service, developed internally by Concentra and hosted on the Microsoft Azure platform.

The following sections provide further detail on the information security and data protection controls we implement to safeguard your data:

Organisation of Information Security

Concentra's commitment to data security and privacy is reflected at all levels throughout the organisation. Concentra has a dedicated Information Security team and Data Protection Officer, with governance in place through an Information Governance Board led by C-Level Executives. An established risk management program is in place with Board level visibility.

Human Resource Security

All Concentra staff are subject to criminal record checks as part of our standard screening process for new employees, which includes extensive background verification of previous employment and educational certificates. Formal Information Security is mandatory for all staff and delivered through an online LMS platform. Awareness training is complemented through company presentations, newsletters and induction sessions.

Asset Management

Within Concentra, owners of physical and information assets are recorded with clear responsibilities outlined. These responsibilities include management of access to information assets, assignment of information classifications and retention periods.

Access Control

- SupplyVue is a web-based solution with the front end being available and compatible with modern browsers.
- User authentication and authorisation is achieved through local Active Directory integration.
- The solution enforces password complexity requirements. End users of the SupplyVue product complete a multi-factor authentication process as part of the enrolment process and as part of the password reset process.
- SupplyVue user accounts are locked for 15 mins after 3 unsuccessful logon attempts.
- Firewall controls are in place along with SSL encryption and application authentication.
- SupplyVue user sessions are timed out after 20 minutes of inactivity.
- Authentication of administrative users is via multi-factor authentication and access to the underlying hosting infrastructure is via dedicated environment user accounts. Connectivity between Concentra and the Azure hosting environment is via a private ExpressRoute connection.
- From an organisational perspective, Concentra access control changes relating to role moves and departures from the organisation are closely managed, with all access to Concentra's own internal systems removed on date of departure. The principles of least privilege and need to know are embedded in the organisation's access control methodology.

The following sections provide further detail on the information security and data protection controls we implement to safeguard your data:

Physical and Environmental Security

SupplyVue is hosted from Microsoft Azure data centre facilities providing benchmark levels of physical and environmental security controls. From an organisational perspective, Concentra offices are managed with extensive physical security controls which have been independently audited for compliance with the requirements of the ISO 27001 standard.

Information Security Incident Management

Concentra has an established Incident Management process incorporating root cause analysis and corrective action remediation. Incident Managers have direct access to Executive leadership to ensure all appropriate resources are available. Any incident impacting the information security or privacy of SupplyVue data would be reported to our clients within 24 hours of discovery.

Business Continuity

- SupplyVue is hosted from the Microsoft Azure platform which commits to an SLA in excess of 99.5%. To uphold this SLA, Microsoft replicate Virtual Machines within their EU availability zones. In addition, Concentra will configure data backups daily to Amazon S3 storage using a Concentra managed encryption key providing encryption at rest. All data between the Azure hosting environment and AWS is encrypted in transit.
- Concentra install and configure monitoring tools on the underlying infrastructure which not only report on availability but also alert our infrastructure team to critical events and incidents. The Azure platform provide monitoring tools as part of the platform which are configured to monitor availability and capacity metrics. The SupplyVue Data Warehouse layer provides logging on the ETL process used for loading source data. These logs will be monitored and used in the event of a data loading incident.
- Concentra will provide at least 7 days' notice of maintenance affecting the availability of the solution. The exception is 24 hours' notice for Microsoft 'Emergency' or 'Critical' patch updates.
- From an organisational perspective, Concentra has an established business continuity planning strategy and takes a cloud-first approach to its own internal systems, reducing dependency on physical infrastructure and office locations.

Operational Security

- SupplyVue solution administrators are located at the Concentra corporate office located in London, UK.
- SupplyVue has a browser based front end with the application being served from a web server. Web server logs are maintained for a min of 90 days. Administrative access is logged in operating system logs. Periodic reviews of access logs are performed and logs are monitored for critical events.
- Critical hosting infrastructure patches are applied as soon as possible and normally the same day, non-critical patches are applied within 30 days, subject to pre-production validation.
- Patches related to the SupplyVue solution components and underlying technologies are subject to Concentra's internal controls within the existing Development, Quality Assurance and Deployment procedures.
- Support incidents are handled by the Concentra service desk who will assign a reported incident with a unique support number. The service desk will categorise the incident in accordance with incident categories and deliver solutions in accordance with the response times detailed in the SLA.
- Deployment of the SupplyVue solution is managed by the Concentra infrastructure team following a strict change control process requiring management sign off prior to production deployment.
- Customer data is removed permanently on request.

The following sections provide further detail on the information security and data protection controls we implement to safeguard your data:

Systems Acquisition Development and Maintenance

- Concentra manages all SupplyVue code development internally. This approach enables consistent levels of information security throughout an established SDLC process, while remaining agile in providing rapid updates and feature improvements through a DevOps and Continuous Delivery framework. All Developers receive training in secure coding practices which are aligned to the OWASP Top 10 Application Security Risks.
- The SupplyVue solution is developed and maintained by Concentra using a dedicated product development team adhering to secure coding standards and the OWASP principles. The development includes a number of capabilities including Business Analysis, Development, Data Analytics, Quality Assurance and Project Management.
- The solution is developed using a number of software components as covered previously in this document. The technology stack includes the Microsoft .Net framework which is a well-known and robust development framework with excellent support.
- Concentra commit to carry out Independent Penetration testing against the solution on a regular basis and provide a management summary to our clients.
- Concentra maintain a comprehensive Application Lifecycle Management process for the SupplyVue solution including the provision of environments dedicated to Development, Quality Assurance, User Acceptance Testing and Production. Concentra will not utilise customer data in any pre-production environment without prior permission confirmed in writing.
- Concentra operate a strict change control process for the SupplyVue product where all changes require approval from the project board prior to implementation. Several quality gates are in place during the development lifecycle.
- Concentra use Distributed and Centralised Source Code Control Systems including DVSC (Git), which means copies of repositories are both distributed among the development team and centralised on a server repository which is backed up offsite on a daily basis and securely stored in encrypted form

SupplyVue Architecture

The SupplyVue solution is hosted in a multi-server environment separating data warehousing functions from user management/authentication, front end data visualisation and user experience. The infrastructure consists of the following components

- Web Portal
- Main Data Warehouse
- Data Loading
- Data Visualisation
- User Management and Authentication
- Perimeter Security

The SupplyVue solution utilises a number of commercial components including the following

- Tableau
- Microsoft SQL Server
- Microsoft Active Directory
- Microsoft Internet Information Server (IIS)
- Microsoft ASP.Net
- Clickatell SMS Gateway

Compliance

- Concentra is registered under the Data Protection Act with the ICO.
- SupplyVue is not designed for the storage of personally identifiable information (PII) or payment card information (PCI-DSS) and we advise this information is removed from any dataset prior in upload.
- Concentra is ISO27001:2013 and CSA STAR (Cloud Security Alliance) certified.
- The production environment will be hosted on the Microsoft Azure platform. Azure meets a broad range of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards including UK G-Cloud. Microsoft was also the first to adopt the uniform international code of practice for cloud privacy, ISO/IEC 27018, which governs the processing of personal information by cloud service providers (CSPs). Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.