# security provisions

## 1. Introduction

1.1 These Security Provisions apply to the provision of Orgvue when ordered by the Customer.

1.2 The Customer acknowledges that the Software together with the Customer Data is, at the Customer's selection, hosted by the Subcontractor in the European Economic Area ("EEA"), North America or Australia. Supplier will not transfer Customer Data outside of the Customer's selected region without prior written instruction from the Customer.

1.3 The Software is multi-tenanted. Customer Data is logically segregated and Encrypted both in transit and at rest.

## 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 **Business Continuity Plan**: Documented strategy identifying risk scenarios which could impact the ability of Supplier to maintain normal business operation, while defining Supplier's response to managing those scenarios.

2.2 **CREST**: A not-for-profit accreditation and certification body providing internationally recognised accreditation for providers of penetration testing services.

2.3 **Data Breach**: A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored, or otherwise processed.

2.4 **Disaster Recovery Plan**: Supplier procedures to enable the recovery or continuation of technology infrastructure and systems required to deliver the Software.

2.5 **Encrypted or Encryption**: The process by which Customer Data is converted into ciphertext to ensure secure transmission or storage.

2.6 **IP Whitelisting**: a security feature used to limit and control access from trusted IP addresses only.

2.7 **Logs**: logs record the outcome of every operation, inclusive of authentication and authorisation failures, by user identity, time and IP address, providing its owner or admin with an audit log of all changes, identifying who made each change, when, and the content of the change.

2.8 **Multi-factor authentication**: an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

2.9 **Multi-Tenanted**: A single database architecture is shared by multiple Customers, in which encryption methods are used to logically segregate and encrypt Customer Data.

2.10 **OWASP Top 10**: is an awareness document for software developers and web application security, identifying the most critical security risks to web applications.

2.11 **SAML 2.0**: Security Assertion Markup Language 2.0 is a version of the SAML standard for exchanging authentication and authorisation identities between security domains

2.12 **Supplier Administrators**: Supplier workers administering and supporting the infrastructure in provision of the Software.

2.13 **Virtual Private Cloud (VPC)**: A cloud computing service that provides users with a virtual private cloud through the provision of a logically isolated section of a public cloud service provider's network.

## 3. Information Security Policies

3.1 Supplier maintains a suite of information security policies which together form an Information Security Management System ("ISMS"). These policies are reviewed at least annually.

3.2 Supplier has an established management framework to initiate and control the implementation and operation of information security within the organization. This includes the allocation of resources necessary to operate, govern and continually improve the Information Security Management System.

## 4. Human Resource Security

4.1 Supplier ensures all new employees and contractors are subject to background checks. These include:

4.1.1 A criminal record check;

4.1.2 Identity and right to work checks;

4.1.3 Professional references from at least two previous employers;

4.1.4 Proof of education and professional certifications.

4.2 Supplier ensures its employment contract includes confidentiality and intellectual property clauses as standard.

4.3 Supplier ensure all employees are assigned mandatory information security training at the start of their employment and are subject to formal annual information security refresher training.

4.4 Supplier maintains a formal employee disciplinary policy, the scope of which includes breach of information security policies.

## 5. Asset Management

5.1 All Customer Data is processed within the Customer's Tenant, unless otherwise agreed in writing from the Customer.

5.2 Supplier will not remove Customer Data from the Tenant without prior written instruction from the Customer.

5.3 Supplier will not process Customer Data on USB media.

5.4 Supplier will implement and maintain up-to-date physical and technical security controls to prevent the use of removable media storage devices

5.5 Supplier maintains an asset inventory of all component systems used to process Customer Data.

5.6 Supplier maintains an Information Classification, Labelling and Handling Policy. This policy applies the most sensitive classification to all Customer Data.

5.7 Within three (3) months of the Agreement termination date, Supplier will securely delete all Customer Data, in such a way that Customer Data will no longer be recoverable.

5.8 Supplier will provide written confirmation of the destruction of Customer Data on written request.

5.9 The Customer may export or delete Customer Data at any time through the Software.

5.10 The following controls will be in place at all times at Subcontractor data centre facilities:

5.11 All decommissioned hardware utilized in the processing of Customer Data will be sanitized and physically destroyed in accordance with industry-standard practices.

5.12 Fire detection systems will utilize smoke detection sensors in all data centre environments.

5.13 Data centre electrical systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Uninterruptible Power Supply (UPS) units will provide back-up power in the event of an electrical failure for critical and essential loads in the facilities.

## 6. Access Control

6.1 Supplier maintains an organisational access control policy to govern access to Supplier systems, including those which process or support the processing of Customer Data.

6.2 Access right authorisation will be subject to a formal process, following the principle of least privilege.

6.3 Supplier ensures that Supplier employee accounts are disabled within 24 hours of employment termination date.

6.4 Supplier ensures that Multi-factor authentication is in place for all access by Supplier Administrators to Supplier systems processing Customer Data.

6.5 Supplier provides support to enable Customers to implement Single Sign-On (SSO) for authentication to their Tenant.

6.6 The Software supports role-based access control models. The allocation of user privileges to the Software must be managed via the Software and is not supported through SAML integration.

6.7 Supplier employees will not access Customer Data without the prior written authorisation of the Customer.

6.8 The Customer is responsible for all User Management including:

6.9 The set up and ongoing management of all users access to the Tenant.

6.10 Ensuring users are granted appropriate permission to access the Software and Customer Data.

6.11 Ensuring access privileges are removed from those users who are no longer authorised to access the Software, for example as a consequence of leaving the Customer's employment or moving department.

6.12 Managing and assigning workers from Supplier who may be required by the Customer to assist on specific engagements. Such Supplier worker access is solely the responsibility of the Customer to control.

## 7. Cryptography

7.1 All Customer Data transmitted over any network is Encrypted using TLS 1.2 or better.

7.2 All Customer Data is Encrypted at rest using AES-256.

7.3 For management of encryption keys used to encrypt Customer Data, Supplier will use the AWS Key Management Service (KMS) which stores and generates master keys on FIPS 140-2 validated Hardware Security Modules (HSMs).

7.4 Master keys will only be used inside these HSM devices and the master keys will never leave such devices unencrypted.

7.5 Master keys will be rotated annually.

## 8. Physical and Environmental Security

8.1 In relation to the subcontractor's datacentres, Supplier shall ensure that the subcontractor:

8.1.1 Controls and restricts physical access to areas where Customer Data is stored to authorised personnel, utilising full authentication controls to validate access (e.g. access control cards).

8.1.2 Promptly revokes physical access rights when no longer required

8.1.3 Requires authorised personnel to utilise multi-factor authentication mechanisms to access hosting data centre floors.

8.1.4 Securely maintains audit trails (including access dates and times) of all access to data centre floors.

8.1.5 Monitors all physical ingress and egress points of data centre points utilising video cameras and recording devices. Recordings shall be stored by the subcontractor for a minimum of 10 working days.

## 9. Operations Security

9.1 Supplier shall ensure that:

9.1.1 Weekly reviews of operating system and web application vulnerability scans are conducted.

9.1.2 Production, testing and development environments are logically separated.

9.1.3 Production Customer Data is never processed in non-production environments.

9.1.4 Server instances processing Customer Data will have active anti-malware services and host-based IDS (Intrusion Detection Services).

9.1.5 Customer Data will be subject to daily backup and retained for 30 days, within the same geographical region as the Customer's Tenant.

9.1.6 Customer Data processed in backup services will be encrypted at rest via AES-256.

9.1.7 Software Logs are retained within the Tenant, with access to the Logs controlled by the Customer . These Logs are retained for the lifetime of the Tenant.

9.1.8 Supplier will collect, consolidate, and review security event Logs from server instances and infrastructure services involved in the provision of the Software. These Logs will not contain Customer Data and shall be retained for a minimum of 12 months. Such Logs are not available to the Customer due to the multi-tenant architecture of the Software. Appropriate summary information may be made available in the event of a Data Breach.

9.1.9 Server instances processing Customer Data will have security patches installed within two weeks of vendor release.

9.1.10 Security patches which Supplier deems emergency and/or critical will be installed to address immediate threats on an expedited basis, according to the severity of the threat.

## 10. Communication Security

10.1 The Supplier shall ensure that:

10.1.1 The public cloud service provider network for the Software is isolated via multiple independent VPCs (Virtual Private Clouds) interconnected via VPC endpoints and exposing only HTTPS TLS 1.2 or better to the public internet for Customer facing services.

10.1.2 A threat detection service with automated alerting to supplier administrators operates on the Software using machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.

10.1.3 Customer Data is not transferred via Email.

10.1.4 IP Whitelisting is supported to restrict traffic to Orgvue from trusted source networks as identified by the Customer.

## 11. System Acquisition, Development and Maintenance

11.1 Supplier maintains an organisational software development policy to govern the development and maintenance of Software. This policy is available to the Customer on written request.

11.2 Supplier Administrators have access only to the necessary source code repositories to support the work they are active on. Identity and Access Management (IAM) roles are used by the build and configuration management services for provisioning and maintenance.

11.3 Supplier shall complete static and dynamic source code analysis in combination with manual code reviews and approval.

11.4 Supplier shall ensure all Software releases pass through logically separate quality assurance and staging environments, before being released into production.

11.5 Supplier shall subject = Software to independent web application penetration testing at least annually. Tests are conducted by CREST certified external resources. An executive summary of these reports is available to the Customer on written request.

11.6 All Software development is aligned to OWASP Top 10 documentation and guidance.

## 12. Supplier Relationships

12.1 All third party suppliers are subject to information security risk assessments and approval before onboarding. Supplier shall monitor and reassess all third-party suppliers on an on-going basis.

12.2 Formal agreements including confidentiality obligations, are included in all Supplier agreements.

## 13. Information Security Incident Management

13.1 Supplier maintains a formal incident management policy incorporating root cause analysis and corrective action remediation. Such incident management policy is available to Customers on written request.

13.2 In the event that Supplier experiences a Data Breach affecting Customer Data, Supplier shall notify the Customer within 24 hours after Supplier becomes aware of the Data Breach and shall instigate its formal incident management policy. In the event of any Data Breach, Customer shall have sole control over the timing, content and method of notification to its employees, Customers and third parties.

## 14. Information Security Aspect of Business Continuity Management

14.1 Supplier shall maintain a Business Continuity Plan for restoring critical business functions, including availability of Software and Customer Data. This policy is available to Customers on written request.

14.2 Supplier shall test its Business Continuity Plan on an annual basis.

14.3 The Software is hosted in a highly resilient public cloud service provider infrastructure, providing geographical data centre fault tolerance. Failover between data centres is automated.

14.4 Supplier will be responsible for backup and preservation of Customer Data. All backup copies of Customer Data shall be treated as Customer Confidential Information and will be encrypted at rest via AES-256 (GCM).

14.5 Supplier will maintain a Disaster Recovery Plan and perform disaster recovery restore testing on a six-monthly basis.

## 15. Standard / Certifications

15.1 Supplier will maintain and provide upon request attestations of compliance with the following certifications, guidelines, attestation, and other standards:

- SOC2 Type 2 annually, covering the previous 12 month period. The SOC2 Type 2 report will include auditor findings and notes. The scope of the SOC2, Type 2 report must include the Software.
- ISO 27001:2013 or more recent version of ISO 27001. The scope of the certification will include the Software.
- ISO 27018:2019 or more recent version of ISO 27018. The scope of the certification will include the Software.
- CSA STAR Level 2. The scope of the certification will include the Software.

## 16. Audit

16.1 Supplier agrees the Customer may, upon reasonable prior written notice, perform vulnerability assessments using industry standard tools and manual techniques to assess the security of Software provided by Supplier in connection with the services provided to the Customer. Customer agrees, in relation to vulnerability assessments it conducts, that the following shall apply. Assessments:

16.1.1 Shall be limited to the Software and not the underlying public cloud service provider services or infrastructure.

16.1.2 Will be performed by authorised cyber security professionals agreed between the parties in advance of the vulnerability assessment taking place.

16.2 The authorised cyber security professionals may work with Supplier to manually validate findings on production and test systems in order to reduce false positives. The authorised cyber security professional(s) may also contact Supplier's designated IT security program manager should any additional information or work be required as part of vulnerability assessment.

16.3 Supplier will be notified by Customer of any major security vulnerabilities without undue delay. Such notice shall summarize in reasonable detail the effect on Customer Data, if known, of the Information Security Incident and the corrective action taken or to be taken by Supplier. Supplier shall promptly take all necessary or advisable corrective actions, and shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate, or rectify such Information Security Incident.

16.4 Upon at least twenty (20) Working Days advanced written notice from the Customer and written confirmation from the Supplier, Supplier shall grant to the Customer (or a third party on Customer's behalf and reasonably approved by Supplier) permission to perform a remote or on-site assessment of Supplier's information security management system, in order to ensure compliance with these Security Provisions. Such compliance assessment will be performed at the Customer's expense, conducted in a way to minimise disruption to the Supplier's business and under the supervision of the Supplier.

16.5 Customer and Supplier will jointly review the completed assessment. If, as part of the assessment, Customer determines changes to be made, then the parties will discuss the proposed changes and associated timeframe for such changes and Supplier will make such changes as are mutually acceptable.