Orgvue Security Overview

Orgvue Security Overview

This document is intended to provide information and assurance on the key information security and data protection controls for Orgvue. Orgvue fulfils compliance with international data protection legislation through a combination of logical controls built-in to the application and those which Orgvue adopts as an organisation.

This document supports our Data Processing Agreement and Security Provisions for Orgvue which can be found at: https://www.orgvue.com/legal/terms-and-conditions/orgvue-subscription-agreement/

Orgvue holds the principle of 'Data protection by design and by default' as a core pillar of its architecture and security posture. As a multi-tenanted environment, orgvue customer data is logically separated and encrypted both in transit and at rest. This is augmented by the access security model for Orgvue which provides customers with control over access to their data, while Orgvue employees will not access customer data without prior written authorisation.

Orgvue is delivered as Software as a Service (SaaS) and hosted on the Amazon Web Services (AWS) platform. Orgvue can be hosted from the AWS us-east-1 (North Virginia), eu-west-1 (Ireland) or ap-southeast-2 (Sydney) Regions. The choice of region is at the discretion of customers.

Orgvue completes a SOC 2 Type 2 report annually and is an ISO 27001, ISO 27018 and CSA STAR (Cloud Security Alliance) certified organisation. The Orgvue application is central to the scope of these assurance programs. Certificates are available at: https://www.orgvue.com/trust-center/compliance/

As a requirement of these international assurance programs, Orgvue has a formal Information Security Policy and maintains a suite of information security policies which form the foundation of our Information Security Management System (ISMS). These policies are reviewed annually.

Orgvue's Information Security team is supported by the Orgvue Information Governance Board. The Information Governance Board meets monthly with membership including the General Counsel, CFO, alongside Information Security and IT leaders. Orgvue has formally appointed a Data Protection Officer.

Orgvue's risk management program is monitored by the Information Governance Board. Quarterly risk assessment workshops are conducted, led by risk owners and the Information Security team.

Remote and mobile working is governed through the **Orgvue Mobile Device and Remote Access Policy**. BYOD for mobile devices is permitted and managed via a Mobile Device Management solution enforcing security controls including encryption, minimum passcode requirements and software versions. No Orgvue data is processed on Orgvue mobile devices.

Human Resource Security

All new Orgvue employees are subject to background checks including a criminal record check as part of the standard onboarding process. Orgvue employment contracts includes confidentiality clauses as standard.

All Orgvue employees are assigned mandatory information security training at the start of their employment. This is further complemented through induction sessions, ongoing annual awareness training, phishing simulations and company presentations. Formal training consists of modules from the SANS Institute, in combination with awareness training relating to company Information Security policies.

Orgvue has a formal Disciplinary Policy, the scope of which includes breach of information security policies.

Asset Management

Orgvue customer data is not processed on USB media, the use of USB removable media storage devices in prevented through logical controls on employee workstations.

On contract termination orgvue data is securely deleted within 90 days and rendered unrecoverable. Written confirmation of destruction can be provided on request. By default, all orgvue customer data is retained for the lifetime of the tenant with customer administrators having the ability to delete their data at any time.

Access Control

Customers are responsible for managing access control to their orgvue environments. Orgvue strongly recommends the use of Single Sign-On (SSO), in combination with which Multi-Factor Authentication may be implemented. In managing access control, orgvue customers are responsible for account creation, disablement and access reviews, in line with their own standard Joiner Mover Leaver processes.

Role-based access control (RBAC) is supported within the Orgvue application.

Within the AWS infrastructure environment, IAM (Identity and Access Management) is used with strict policies for segregation of duty, with the principle of least privilege carefully addressed to control Orgvue administrator access to underlying AWS infrastructure. Multi-Factor Authentication has been implemented for all privileged access by Orgvue administrators. As previously stated, these privileges do not include access to customer data.

Orgvue Developers have access only to the necessary source code repositories to support the work they are active on. IAM authentication and roles are used by the build and configuration management services for provisioning and maintenance.

From an Orgvue organizational perspective, access control is formally governed though the **Orgvue Access Control Policy** and complemented by the **Orgvue Password Policy**. Multi-Factor Authentication is in place for domain level authentication. Departing Orgvue employee accounts are disabled on date of departure. The principle of least privilege is enforced throughout the organization and maintained through regular application access reviews.

Data Encryption

All orgvue data is encrypted at rest through the application via AES-256. All orgvue data is encrypted in transit using TLS 1.2 or better.

As a multi-tenanted SaaS architecture, orgvue customer data is logically segregated using separate table namespaces (schemas) per tenant. At the storage layer Orgvue customer data is encrypted at rest via AES-256.

orgvue leverages the AWS KMS (Key Management Service) for key management. **The KMS is designed so that no party can ever access the master keys**. The KMS uses FIPS 140-2 validated hardware security modules (HSMs) to generate and protect keys. Keys are only used inside these devices and can never leave them unencrypted. Master keys are rotated annually.

Physical Security

Orgvue is hosted from AWS data centres. Physical access to areas where orgvue data is processed is controlled and restricted to authorised persons only. Authentication controls are used to authorise and validate all access.

Information on AWS physical security controls is available at: https://aws.amazon.com/compliance/data-center/controls/

For security reasons, AWS do not publish information on the physical location of their data centers beyond the country or state geography. As such, Orgvue is unable to provide this information to our customers.

Operations Security

Vulnerability Management

Container vulnerability management for Orgvue runs as part of the build process. AWS ECR image scanning runs daily, providing static scanning for container images. Agent based vulnerability management is implemented across the Orgvue organization, including corporate server and workstation environments.

Operating System security updates are applied within two weeks of vendor release and applied consistently throughout the orgvue product and corporate environments.

Web application penetration testing for Orgvue is completed annually. The executive summary reports of these tests are available to customers on request.

Intrusion Detection and Endpoint Protection

At the network level, the AWS GuardDuty service is active on the AWS orgvue environment. AWS GuardDuty is a threat detection service which uses machine learning, anomaly detection and integrated threat intelligence to identify potential threats.

Orgvue corporate servers and workstations run full antivirus and endpoint protection solutions. These are updated daily with daily scans in place for all workstations.

Log Management

Orgvue user activity is logged in the application and Event Store. The Event Store holds an immutable log of all data mutations, while the application logs an immutable log of all application events. These logs are retained for the lifetime of the tenant and are stored within the encrypted customer tenant, accessible by customer tenant Administrators only.

Orgvue records the outcome of every operation, inclusive of authentication and authorisation failures, by user identity, time and IP address, providing an audit log of all changes, identifying who made each change, when, and the content of the change. Tenant Administrators can also see 'recent activity' in a dataset.

Orgvue infrastructure security log events are centrally consolidated. Alerts are generated from automated queries in addition to manual review. Logs are retained for a minimum of 12 months. These logs are not available to orgvue customers.

DLP (Data Loss Prevention)

To preserve customer data encryption and in the interests of minimizing Orgvue access to customer data, the Orgvue application does not provide Data Loss Prevention (DLP) services nor monitor file status changes.

From a broader Orgvue organizational perspective, DLP Microsoft Azure tools are active, providing DLP for email and core applications

Communications Security

AWS Architecture

Provisioning and hosting within AWS have been designed to address defence in depth across the entire process from development, test, build, deployment, hosting and maintenance and is subject to continuous review. Secure by Design principles are carefully followed with the goal of minimising the attack vectors exposed.

All assets at rest, application and infrastructure configuration and customer data are encrypted using AES-256 using AWS KMS keys. The network is isolated via multiple independent VPCs (Virtual Provide Cloud) interconnected via VPC endpoints and exposing at least HTTPS TLS 1.2 to the public internet for customer facing services.

Web Application Firewalls (WAF) are in place for Orgvue.

AWS Security Groups are used to segment egress traffic from Elastic Container Service tasks to the AWS ALB (Application Load Balancer). The same tunnelling strategy is in effect from the ALB upwards to a public security group granting access to Port 443 only. Several ALB TLS policies are in place carefully mapping the most secure ciphers available.

Orgvue supports the implementation of IP allow-listing to restrict the IP address ranges from which users are able to connect to the application.

Software Development Security

Orgvue software development security is governed through the **Orgvue Software Development Policy** and aligned to OWASP principles for secure development.

All orgvue releases pass through QA and Staging before being released to Production. Production data is never processed in non-production environments.

Orgvue source code static analysis including software package dependencies, is automated as part of the build process in combination with manual code review and approval. Dynamic code analysis is also completed as part of the release cycle.

Major new orgvue releases are subject to web application penetration testing using independent CREST accredited resources. The executive summary reports of these tests are available to customers on request.

Orgvue Releases are initiated by privileged, non-development members of the orgvue team via the Build Service, requiring multi-factor authentication. Successful builds are hot swap deployed into staging before test and release into production via automation tools using a blue/green deployment strategy with Auto Scaling failover.

Supplier and Third-Party Management

Amazon Web Services (AWS) is the only third party involved in the delivery of orgvue and has no access to orgvue customer data.

New suppliers with access to Orgvue organizational data are subject to information security risk assessments as part of the onboarding process. Existing supplier risks are assessed through the risk management program.

Incident Management

Orgvue 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.

Security incidents are managed through the **Orgvue Incident Management Policy** and **Orgvue Security Incident Handling Policy**.

Orgvue commits to notify customers of security incidents which may impact their data within 24 hours. This is formalized in the standard terms and conditions for Orgvue.

Business Continuity

Orgvue has a formal Business Continuity Policy. Orgvue is hosted on highly available AWS infrastructure leveraging multiple AWS Availability Zones to provide geographical data centre fault tolerance. Multiple AWS data center facilities would need to fail to result in orgvue being unavailable.

Orgvue data is backed up daily and retained for 30 days within the same AWS Region infrastructure where the production service is hosted from. Backup data remains encrypted at rest and highly available. The database restore process for orgvue data is tested on a six-monthly basis.

From an organizational perspective, Orgvue has a cloud-first approach with no reliance on its office locations for systems and services. In the event of a disaster event impacting Orgvue sites, all employees work remotely.

Compliance

Orgvue is compliant with international legislation and data protection laws. As a Data Processor, Orgvue delivers compliance with its GDPR obligations to provide sufficient guarantees in implementing appropriate technical and organisational measures, notably through our SOC 2 Type 2, ISO 27001, ISO 27018 and CSA STAR assurance programs. Certificates are available to download at: https://www.orgvue.com/trust-center/compliance/

Independent third-party reviews of Orgvue's Information Security Management System are completed annually as part of SOC 2 Type 2, ISO27001 and CSA STAR.

Orgvue has an established internal audit program to support compliance with its information security policies and program. The audit function maintains independence from the respective lines of business.

With respect to the AWS hosting infrastructure, information on AWS security compliance standards is available at: https://aws.amazon.com/compliance/programs/

Contact Us

For further information or questions, please contact us at infosec@orgvue.com