orgvue security overview

orgvue: overview of security processes

This document is intended to provide information and assurance on the key 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 Provisions 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 true multi-tenanted environment, each orgvue client tenant is logically separated and uniquely encrypted using a dedicated encryption key, ensuring appropriate technical measures are in place to safeguard your data. This is augmented by our access security model which means that you have exclusive control over access to your orgvue data, while orgvue has no access unless you authorise and engage us to.

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.

orgvue is an ISO 27001, ISO 27018 and CSA STAR (Cloud Security Alliance) certified organisation. As a requirement of these international standards for security, 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, with changes communicated to employees through our online Learning Management System (LMS).

orgvue's Head of Information Security leads the Information Security team, supported by the orgvue Information Governance Board. The Information Governance Board meets monthly with membership including the General Counsel, CTO and CIO and Head of Information Security. orgvue has formally appointed a Data Protection Officer.

orgvue has a Risk Register with formal risk management program in place, monitored by the Information Governance Board. As part of the risk management program, cross functional information security 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. Our employment contract includes confidentiality clauses as standard.

All orgvue employees are assigned mandatory information security training at the start of their employment, delivered by an LMS solution. 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 the assignment of all Orgvue Information Security policies. Training completion is recorded, with compliance status reported to the Information Governance Board.

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

Asset Management

All orgvue client data remains within the secure tenant environment, is not removed nor processed on USB media or other orgvue systems. There are no physical transfers involved. orgvue data is uploaded directly by the client into their orgvue tenant, with the transfer encrypted through TLS 1.2.

On contract termination orgvue data is securely deleted no later than 90 days after termination through destruction of the client tenant encryption key and deletion of the database schema. Written confirmation of destruction can be provided on request. By default, all orgvue client data is retained for the lifetime of the tenant with client administrators having the ability to delete their data at any time.

Access Control

By default, orgvue has no access to orgvue client data, with our clients exclusively responsible for managing access control to their orgvue environments. orgvue strongly recommends the use of Single Sign-On (SSO) to authenticate to orgvue, in combination with which Multi-Factor Authentication may be implemented. SAML 2.0 is supported for SSO. In managing access control, orgvue clients are responsible for account creation, disablement and access reviews, in line with their own standard Joiner Mover Leaver processes.

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 client 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.

Authorization within the orgvue application is managed through support for both Role (RBAC) and Attribute based Access Control (ABAC).

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 with access reviews in place as part of role change. The principle of least privilege is enforced throughout the organization and maintained through consistent application access reviews.

Data Encryption

All orgvue data is encrypted at rest through the application via AES-256 (GCM). All orgvue data is encrypted in transit via TLS 1.2 with (at minimum) 128-bit AES encryption.

As a multi-tenanted SaaS architecture, orgvue client data is logically segregated using separate table namespaces (schemas) per tenant. These client dedicated schemas are individually encrypted via encryption keys unique to each client.

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**.

All orgvue data is encrypted via the AWS KMS at EBS (Elastic Block Storage) and S3 (file storage) levels. A second layer of encryption is enforced at the service layer above the database layer for client data, with tenant dedicated encryption keys sourced from KMS with the master key held within the FIPS-140-2 certified KMS HSM (Hardware Security Module). The cryptographically secure master key is generated within the HSM and is never transmitted externally so that no party can ever access that key. Envelope Encryption (AES-256) is performed at the application layer from data keys (DEKs) generated under the master key (CMK). CMK rotation occurs annually.

Physical Security

orgvue is hosted from AWS data centers. Physical access to areas where orgvue data is processed is controlled and restricted to authorized persons only. Authentication controls are used to authorize and validate all access.

Full 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 clients.

Operations Security

Vulnerability Management

Qualys Cloud Agent and Amazon Inspector are installed on all EC2 VM instances. Vulnerability scans are continuous via Qualys Cloud Agent. These scans are formally reviewed at least weekly by the Information Security team and include web application scanning in combination with OS level scans. The Qualys Cloud Agent solution is implemented across the Orgvue organization, including the orgvue AWS, corporate server and workstation environments, providing near real-time vulnerability information.

Container vulnerability management is implemented on build via JFrog Xray. AWS ECR image scanning runs daily, providing static scanning for container images.

Operating System security updates are applied within two weeks of vendor release and applied consistently throughout the orgvue server environment through an automated build process.

Orgvue completes at least annual web application penetration testing for orgvue using independent CREST accredited resources. The executive summary reports of these tests are available to clients 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.

All orgvue server instances along with all orgvue organizational servers and workstations run full Anti-Virus and endpoint protection solutions. Signatures 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 client tenant, accessible by client tenant Administrators only.

orgvue records the outcome of every operation, inclusive of authentication and authorization 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 clients.

DLP (Data Loss Prevention)

By default, orgvue has no access to orgvue client tenant data, so cannot provide DLP services nor monitor file status changes.

From a wider orgvue organizational perspective, the Microsoft Cloud App Security and Windows Security Centre services are active, providing DLP for email and core cloud-based applications.

Communication Security

AWS Hosting Architecture

Provisioning and hosting within AWS has been designed to address defense 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 minimizing the attack vectors exposed. All assets at rest, inclusive of built AMIs (Amazon Machine Images), application and infrastructure configuration and client data are encrypted using industry standard encryption algorithms using AWS KMS keys. The network is isolated via multiple independent VPCs (Virtual Provide Cloud) interconnected via VPC endpoints and exposing only HTTPS TLS 1.2 to the public internet for client facing services.

AWS Security Groups are used to tunnel egress from server instances to the AWS ALB (Application Load Balancer). The same tunneling 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 client data is not transferred by orgvue over WiFi networks nor email, remaining within the secure tenant environment at all times.

Orgvue supports the implementation of IP Whitelisting to restrict the range of source IP addresses from which users may 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 clients 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 client data.

New suppliers that have access to orgvue organizational data or physical locations 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** which are communicated to staff through our LMS system.

orgvue commits to notify clients of security incidents which may impact their data within 24 hours which is formalized in the standard orgvue terms and conditions.

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 center 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, highly available and backed by AWS SLAs committing to durability of 99.999999999% across multiple Availability Zones.

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 would 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 organizational measures, notably through our ISO 27001, ISO 27018 and CSA STAR certifications.

Independent third-party reviews of orgvue’s Information Security Management System are completed annually as part of the ISO27001 and CSA STAR certification standards.

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

,