Security & Privacy Guide

May 2019

JASK
11501 Rock Rose Ave Suite 200
Austin, TX 78758
1-800-335-0403
info@jask.com
https://jask.com

Table of Contents

Welcome

This guide is an overview of the people, processes, and technology JASK uses to develop, test, and deploy our cloud products.

When evaluating the security of a cloud solution, it is important to distinguish between:

- **"security of the cloud"** - security measures the cloud service that the provider implements and operates.
- **"security in the cloud"** - security measures the cloud user implements and operates, related to the security of applications using AWS services.

JASK uses Amazon Web Services (AWS) as our cloud hosting provider. AWS shares responsibility with JASK for the security of cloud operations. AWS provides "security of the cloud" while JASK provides "security in the cloud." AWS publishes substantial documentation on their security best practices.

This guide describes JASK's security procedures in five areas:

- How we protect your data
- Our operational security procedures
- Our secure development practices
- Our organizational security program and policies
- Privacy and compliance considerations

Security does not end with JASK. Your team also shares responsibility for security. AWS is responsible for the security of their infrastructure, JASK is responsible for the security of the JASK application(s), and you are responsible for the security of your accounts. Your team should choose strong passwords, enable two-factor authentication for all users, and carefully protect email accounts to reset forgotten passwords. You should also review your internal data classifications and have a good understanding of what types of (regulated) data might be within your environment and processed by JASK.

JASK's operations are covered by a SSAE-16 SOC2 Type 1 report ("SOC 2"). SOC 2 reports are developed and governed by the American Institute of Certified Public Accountants. The reports are similar in structure to financial audit reports, except that they focus on technical controls instead of on financial controls. It is an industry standard that is used to validate the security controls to manage the confidentiality, integrity, and availability of cloud infrastructure and customer data. Our services have an AICPA SSAE-16 SOC 2 Type 1 Report, as described by Attestation Standards Section 801. This report is available upon request.

If you have questions that are not covered in this guide, contact your JASK account representative or email us at info@jask.com. Due to the evolving nature of threats and business needs, JASK reserves the right to modify our practices.

Secure Data

In the world of the cloud, “data security” has different definitions for different people. This section
covers data security from the following four perspectives:

- **Physical** - where your data is physically located.
- **Political** - the political environment where your data and data-controlling entities reside.
- **Legal** - the legal entities that control or process your data.
- **Logical** - which people and networks have access to your data.

JASK services are hosted in the following locations:

- Oregon, United States (AWS us-west-2)
- Canada (AWS ca-central-1)
- Frankfurt, Germany (AWS eu-central-1)

During provisioning, JASK allows you to choose the AWS location that hosts your service and your data. JASK will never move your data from the selected region unless specifically requested to do so by the customer.

Physical Security

AWS data centers are staffed 24x7 by trained security guards. Data center access is authorized strictly on a least privilege basis. AWS customers are not authorized physical access to any AWS data center. Physical controls in AWS data centers are validated by auditors as part of AWS’s SSAE-16 SOC 2 Type II report. Independent reviews of these physical controls is included in AWS ISO 27001 audit, the PCI assessment, ITAR audit, and FedRAMP testing programs. See the AWS Risk and Compliance Whitepaper for information about AWS physical security.

Political & Legal

Neither AWS nor JASK will disclose your data unless required by law, regardless of the applied source or type of political pressure. Both AWS and JASK policy will notify customers before disclosing their data, unless we are legally prevented from doing so.
See Amazon Web Services Data Privacy FAQ for more information on AWS data privacy policies.

JASK does engage other third party services providers. Before engaging such providers, JASK

conducts review of service provider's security, privacy and confidentiality practices, and contractually imposes JASK's standard security and privacy requirements as required by applicable laws.

Logical

JASK's production infrastructure is an independent security and administrative domain from JASK's internal IT systems. Administrator access to either domain does not mean access to the other. Similarly, if JASK's internal IT systems are compromised, it does not enable lateral movement into another our production infrastructure. JASK's production infrastructure is further segmented, based on the service requirements and the principle of least privilege.

Access controls

Access to data requires access to the systems on which it is processed. Access is permitted via the operating system of the machine that processes the data or the JASK application. Only JASK authorized personnel have access to production systems where customer data is stored. All access is via secure shell, authenticated per-user, and requires a username, password, SSH public/private keys, and a two factor authentication token. Role based access controls, audit logging and the theory of least privilege are used to provide logical segmentation and tracking of user behavior on assets in which each user is permitted. Network access to systems is restricted via comprehensive network controls.

Encryption

The data from your on-premise devices to JASK is encrypted in transit by using Transport Layer Security (TLS). JASK closely monitors industry best practices for TLS configurations and makes sure that our products enforce appropriate protocols and ciphers. Any data transmission via unsecured transports is not supported and is strictly prohibited.

All customer data is stored in AWS S3 buckets and encrypted at rest with AES-256 via AWS's SSE-S3.

Data segmentation & destruction

JASK uses a single-tenant storage & multi-tenant data processing model. Single tenant storage ensures your data is clearly segmented into a logical boundary with dedicated security controls, independent of all JASK application code. Multi-tenant data processing maximizes the efficiency of compute resources and keeps your costs low. All data processing services are stateless and only operate on one customer's data at a single time. Data is never commingled, in either processing or storage.

Secure Operations

Audit Logging & Retention

Role-based access controls, audit logging, and the theory of least privilege are used to provide logical segmentation and tracking of authorized user behavior on all JASK production systems. These logs are transmitted in real time to a central logging system and are retained for 12 months.

Security Monitoring

JASK staffs a 24x7x365 Cloud Security team with analysts to investigate any unusual activity. These analysts receive security alerts and respond as needed. Any abnormal activity is escalated to Tier II responders for deeper investigation and response.

Third-Party Penetration Tests

JASK's AWS infrastructure undergoes annual network penetration tests by a third-party security firm to validate our configuration management procedures. Evidence of the most recent penetration test is available upon request.

Secure Network, Operating System Configurations and Patch Management

Public services are limited to TCP/80 and TCP/443 (HTTP and HTTPS). HTTP simply redirects to HTTPS. Management access for administration is limited to the small number of operations staff who are directly responsible for managing the service's infrastructure. Operating system configurations are tightly controlled and hardened. In addition to the security risk of unnecessary services, they also present availability and performance risks. Thus, we carefully limit operating system services to those services critical to the function of the operating system and our application.

Patches are applied regularly as part of the routine operations and updates to the systems; exception procedures are in place for critical patches that require immediate application to maintain optimal security.

Vulnerability Scans

JASK uses a variety of automated vulnerability scanning & management platforms to monitor systems for unexpected configuration changes and vulnerable software packages. These platforms run at least monthly. Many are in constant use and proactively deliver alerts to the Cloud Security team in near real time.

Backups and availability

JASK's cloud architecture is architected for highly available service: all services use resources in at least two data centers in your selected region. Data is replicated in real time between data centers, with seamless failover between service data centers. Loss of a system or disk does not result in service interruption or data loss. Loss of an entire data center does not result in service interruption or data loss.

JASK tests failover and restore procedures as a part of day-to-day operations. Upgrade procedures failover services as part of each upgrade: the same as if there were complete loss of a data center.

In the unlikely event the service is unavailable, all JASK sensors cache data until the server becomes available. Service downtime does not result in data loss unless the volume of data exceeds the local cache configuration.

Change Control

JASK's product operations teams follow "Infrastructure as Code" development principles.

When infrastructure is code, it is checked into a source code repository. Proposed changes are tracked on a per commit basis, and each commit includes a brief message with context, including a link to a ticket. Each change goes through a manual code review process, which includes automated functionality testing, source code security analysis and other checks used as a conditional acceptance before review by other members of the team. Merging code is not authorized until at least one other individual has approved the change.

These procedures mirror those of the traditional software development processes, allowing consistent procedures and practices between application development and infrastructure management within the team. These practices are a core tenant of "DevOps."

As a result, all changes to production infrastructure:

- Are saved as a clearly-defined changeset in a source code repository with metadata that includes who made the change, when, why, and a reference to a ticket that is used to coordinate the change.
- Each proposed change undergoes automated acceptance testing, including QA tests and security-specific tests, static and dynamic code analysis.
- All proposed changes that pass acceptance testing must pass code review by at least one additional engineer who has sufficient knowledge of the system.
- Any security-sensitive changes must pass code review by the team's designated security Engineer.
- Both regular and security engineers have escalation procedures to senior members of the architecture and security teams to escalate change reviews as needed.

These change control procedures are backed up by vulnerability scanners and configuration monitors that alert on unexpected or unsafe changes to critical configurations. If an unsafe change passes each of these controls and still makes it to production, it triggers a root cause analysis of the control efficacy. The review team makes recommendations for control updates to mitigate the risk of that change happening again (such as training, education, new automated tests or architectural update).

More information on the JASK Secure Development Lifecycle is available in the Secure Development section below.

Denial of Service

Every Denial of Service (DoS) attack is unique and the solution is tailored to the attack.

AWS uses proprietary techniques to mitigate the risk and reduce the impact of many off-the-shelf Distributed Denial of Service (DDoS) attacks. In the event of an attack, JASK personnel will actively work with AWS staff to develop countermeasures specific to the attack profile. This can be simple IP filtering, specialized proxy servers in front of the server, deep packet inspection, or any combination of these measures.

Secure Development

The JASK Product Security Program is a set of activities to secure our products through their lifecycle from planning to development and deployment. It includes three primary components:

- **Product Risk Management Plan**: a bottom up evaluation of the risks to product security, the mitigations in place to reduce risks and the areas we are investing to further reduce risks within our products.

- **Secure Development Lifecycle**: activities during software development required to ensure security is deliberately considered during the planning, development and release testing.
- **Security Response Center**: monitoring for and responding to vulnerabilities in our products post-release.

Product Risk Management Plan

The risk management plan defines why we invest in product security. It reviews the risks related to our products, mitigations in place to reduce those risks and the resulting residual risks. It aligns all stakeholders on the management plan for those risks. The resulting security management philosophy is clearly communicated to engineering to enable wise implementation decisions. In an industry where customers rely on products to improve their own security posture, these are critical activities.

Development and management of the risk management process is a high-level and iterative approach, deeply integrated through the software development lifecycle. There are three goals:

- identify, rank, track and understand risks to product security
- identify operational activities in place to mitigate risks
- accept residual risks too low priority or too costly to mitigate

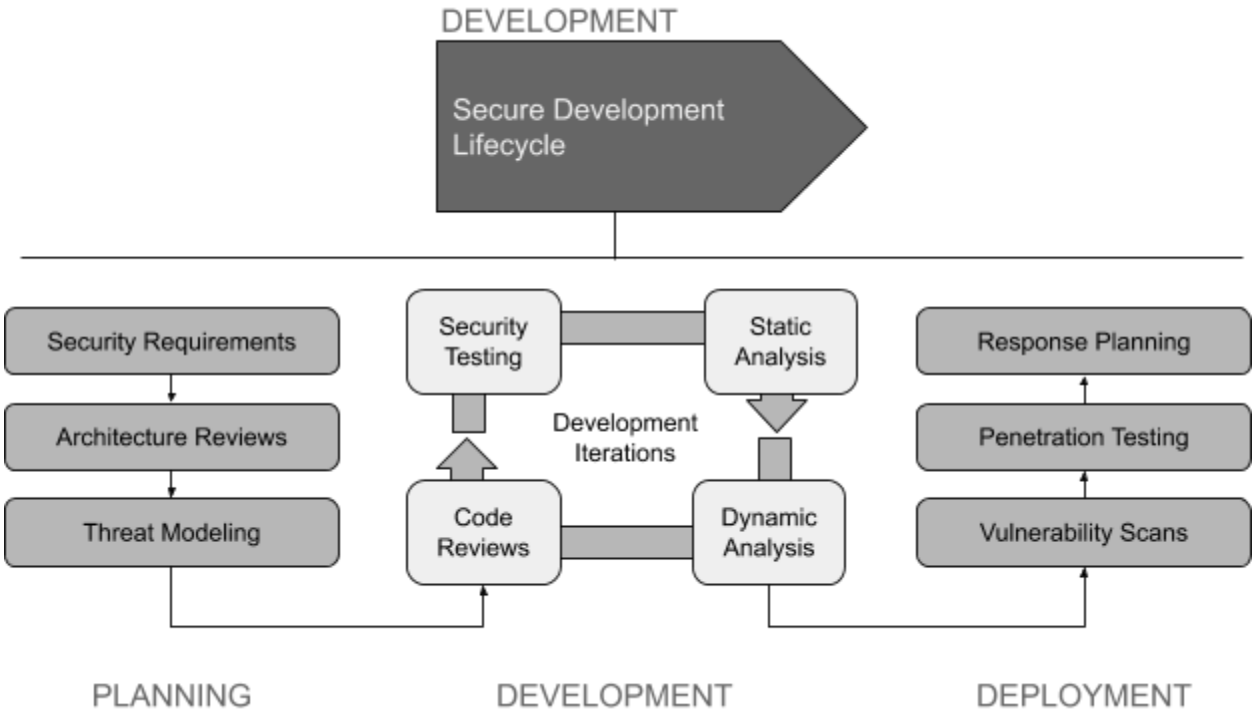
The Risk Management Plan is distinct from threat modeling or architecture reviews. Those activities are part of the Secure Development Lifecycle and apply the business's risk management philosophy to new development. They are executed by the development teams, derived from the guidance in the business’s Risk Management Plan, and ensure consistency across the product teams.

The product teams develop JASK's Risk Management Plan with support from the product security group. The plan is renewed, reviewed and approved by JASK's executive team every year.

Secure Development Lifecycle

JASK's Secure Development Lifecycle (JSDL) is designed to identify and mitigate product security risks during the product development phase. The JSDL is heavily influenced by industry best practices such as Microsoft's Security Development Lifecycle, SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model). It is a collection of activities executed during the development process to ensure security during all development phases and include:

- Planning Phase
  - Security Requirement Review
  - Architecture Reviews
  - Threat Modeling
- Development Phase
  - Code Reviews
  - Static Analysis
  - Dynamic Analysis
  - API and UI Automated Scans
- Release
  - External Vulnerability Scans
  - Penetration Testing
  - Security Response Planning and Coordination



The rigor of our process attempts to prevent vulnerabilities from ever being introduced. It is evaluated regularly throughout the year to continue improving the security posture of our development practices.

Security Response Center

The JASK Security Response Center (JSRC) manages security vulnerabilities in JASK products after release. The JSRC receives product vulnerability reports from researchers, customers, partners, as well as through internal and third party testing. The JSRC will validate the report, communicate to the reporter (if necessary) and queue the reported vulnerability for resolution. After each report is validated and remediated, JSRC will communicate vulnerability details including severity, criticality, and any available workarounds and remediation procedures to customers via security advisories.

Our overarching goal as an organization is to ensure our customer's endpoint security is improved by the use of our products and any vulnerabilities which impact that goal are treated with urgency and transparency.

Secure Organization

JASK maintains a library of policies and procedures related to information security and privacy. These policies are reviewed and refreshed at least annually. They are provided to employees during the hiring process as part of initial training and are always available online.

JASK does not distribute these policies. As part of our SSAE-16 SOC2 assessment, our auditors have reviewed these policies to ensure their suitability. Summaries of the SOC2 reports are available upon request.

Personnel Security

Background checks

Every JASK employee and contractor undergoes a background screening during the hiring process. Background checks for US personnel include:

- 7-year criminal history search at federal, state and county levels (county availability is state dependent)
- Social security trace
- Widescreen Plus National Criminal Search
- Social security validation

The background screening must be completed with no material findings before an employee's start date or contract start.

Confidentiality Agreements

Every JASK employee's employment agreement includes confidentiality clauses that explicitly describes and legally protects customer/confidential data. Any raw or attributable data from our customers is considered Customer Data and is subject to usage that is described in the applicable license agreement. Any agreements with third-party service providers also include confidentiality clauses.

Acceptable Use and Code of Conduct

All JASK employees are bound by the JASK Code of Business Conduct and Ethics that describes the behaviors that our culture demands. It also describes an Acceptable Use policy (also applicable to contractors) that describes appropriate use of our information and information systems.

Security Policies

In addition to the Acceptable Use policy, JASK maintains detailed security policies that describe appropriate use of our information systems, specific to security concerns. Employees and contractors are required to review and acknowledge the security policies annually.

Security Training

Every JASK employee undergoes security training both at the time of hiring and annually. Training content is refreshed each year to reflect current threats and trends in the security industry. Employees are required to acknowledge that they understand their responsibilities in the security of our systems.

Business Continuity Management

JASK's cloud services are architected to be highly available and minimize or eliminate single points of failure. As described in detail in the preceding backup section, service architecture follows modern cloud application practices to use resources at multiple physical data centers in separate geographic locations, to make sure that the service remains available.

Additionally, our production cloud service is an independent administrative domain logically isolated from JASK's internal office automation and IT systems. For example, failure of JASK's email server or a file server does not impact your service. Internally, each service is architected to further isolate failure domains and limit the impact of failure as much as is practical.

JASK's Corporate IT services for critical business processes are similarly architected to eliminate or reduce single points of failure in technical systems and personnel. In general, JASK

uses cloud services for all business-critical activities such as communication and processing systems. JASK does not maintain its own data center which means we have no dependence on any single physical location.

Regulatory Compliance

General Data Protection Regulation (GDPR)

Processing personal data to ensure enterprise network security is broadly recognized as a "legitimate interest" under the GDPR. Recital 49 of the GDPR says that every data controller has a legitimate interest in:

> *"the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity and confidentiality of stored or transmitted personal data. And the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams, computer security incident response teams, by providers of electronic communications networks and services and by providers of security technologies and services."*

JASK's platform is aimed at allowing your security team to prevent unlawful or malicious actions to your enterprise networks. Please consult your privacy advisor for proper classification of the legal basis under the GDPR before deploying JASK.