# Security and Privacy Guide

September 2024

Sevco Security, Inc.
www.sevcosecurity.com
support@sevcosecurity.com

## Revision History

| Revision date | Items revised | Author |
|---|---|---|
| 21 September 2021 | Approved | James Darby |
| 15 July 2022 | Reviewed | James Darby and Kenyon Sutherland |
| 24 Sep 2024 | Reviewed and updated Physical Security | Kenyon Sutherland and Troy Reish |

# Table of Contents

# Introduction

This guide is an overview of the people, processes, and technology Sevco Security Inc. (***"Sevco", "us" or "our"***) uses to develop, test, and deploy our products and services (***"Services"***).

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

- **"security of the cloud"** - security measures that the cloud provider implements and operates.
- **"security in the cloud"** - security measures the cloud solution vendor implements and operates, related to the security of its applications.

Sevco is directly responsible for providing "security in the cloud" for the Services it provides.. Sevco uses Amazon Web Services (AWS) and the Google Cloud Platform (GCP) as our cloud hosting providers and consequently, rely on each for "**security of the cloud**" operations. Both AWS and GCP publish a Shared Responsibility Model for guidance on security best practices.

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

- **Secure Data -** How we protect your data
- **Secure Operations -** Our operational security procedures
- **Secure Development -** Our secure development practices
- **Secure Organization -** Our organizational security program and policies
- **Privacy & Compliance** - Privacy and compliance considerations

Security does not end with Sevco. Your team also shares responsibility for security. You are responsible for the security of your accounts.

Your team should enforce and follow best practices, including choosing strong passwords, enabling two-factor authentication for all users, and carefully protecting internal email accounts to ensure secure resetting of forgotten passwords.

If you have questions that are not covered in this guide, contact your Sevco representative or email us at support@sevcosecurity.com.

Due to the evolving nature of threats and business needs, Sevco reserves the right to modify our practices and policies.

# Secure Data

Sevco uses Amazon Web Services (AWS) as our cloud hosting provider. Sevco leverages the AWS security regime, as well as Sevco's own internal data security practices, to deliver Sevco Services to our customers.

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.

## Physical Security

Sevco's Services are physically hosted in:

- AWS in the US-East Region, Northern Virginia,  USA
- GCP in the US-East4 Region, Ashburn, Virginia, USA

These datacenters are staffed 24x7 by trained security guards. Datacenter access is authorized strictly on a least privilege basis. Customers are not authorized physical access to any datacenter. Physical controls are validated by auditors as part of SSAE-16 SOC 2 Type II report for AWS and GCP. Independent reviews of these physical controls are included as part of ISO 27001, PCI, ITAR and FedRAMP testing programs. See the Risk and Compliance Resource Centers for AWS and GCP for more information on physical security.

## Political & Legal

Sevco will not disclose your data unless required by law, regardless of the source or type of political pressure. It is Sevco policy to notify customers before disclosing their data,  unless we are legally prevented from doing so.

In providing Services, Sevco can engage other third party services providers, such as AWS & GCP. Before engaging such providers, Sevco conducts a review of the service provider's security, privacy and confidentiality practices, and contractually imposes Sevco's standard  security and privacy requirements as required by applicable laws. Please visit our privacy policy for up to date information.

See Amazon Web Services Data Privacy FAQ and Google Cloud Privacy Notice for detailed information on their data privacy policies.

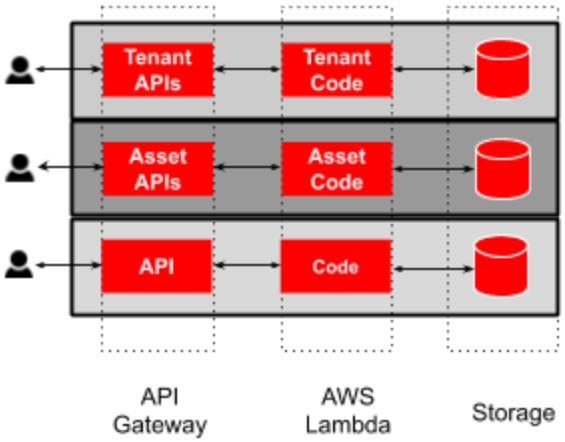
# Logical

This section describes the logical controls of your data in four categories:

- **Data Architecture -** how the platform processes and stores your data
- **Data Access** - the controls in place around who and what can access your data
- **Data Protections** - the encryption and segmentation controls in place for your data
- **Data Segmentation and Destruction** - how your data is segmented from other clients and destroyed

## Data Architecture

Sevco's cloud platform follows the "serverless" architecture design using AWS's API Gateway service, Lambda service and various storage services. APIs are grouped by "family," and each API group manages its own resources, independent of all other services.




Each API group runs inside a dedicated virtual network and uses AWS's Identity and Authorization Management system to control access to resources. The IAM permission system follows the principle of least privilege, ensuring every resource has permissions to access only exactly what it needs based on the processing needs.

## Access Controls

All access to your data is controlled by AWS's IAM system in one of AWS's managed storage services. Access is limited to the AWS Lambda function responsible for processing the data relevant to the API group.

A subset of Sevco staff requires access to those data storage services for monitoring and troubleshooting. The access is limited to Sevco personnel responsible for managing production systems. All access is authenticated per-user, uses role-based access controls to limit access and requires a two factor authentication token.

Sevco also runs both demo and dev environments for day to day operations. These environments do not contain production customer data and allow broader access to systems for routine research and development tasks, further limiting the need for staff to access production systems. All deployments, from dev to demo to prod, use automated deployment procedures, ensuring no humans have to be involved in the updates, again limiting staff required to access production systems.

## Data Protections

All data to, from and within Sevco is encrypted in transit by using Transport Layer Security (TLS). Sevco 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.

Your data is encrypted at rest anywhere it is persisted using AWS's storage service encryption technologies.

## Data Segmentation & destruction

All Sevco data is grouped by "Organization" or "tenant." When any customer establishes service with Sevco, it creates a new Organization. This represents the primary data security boundary for all data within an Organization. While there are access controls within an organization for your users to have access appropriate for their role, those are administrative controls rather than security controls.

All Sevco data processing is single-tenant. Every AWS Lambda function operates on one tenant at a time and all data, when stored, must be accompanied by the Organization Identifier ("org id") the data originated from. Every API request must contain the desired org id and those are encoded in the user's authentication token based on the organization the user account is defined to.

Finally, your data is destroyed in one of two cases: at the end of the defined retention period (typically less than 90 days) or on contract termination when the Organization containing your data is deleted.

# Secure Operations

## Audit Logging & Retention

Role-based access controls, audit logging, and the policy of least privilege are used to provide logical segmentation and tracking of authorized user behavior on assets. These logs are transmitted in real time to AWS CloudTrail's logging system and are retained for 90 days.

## Security Monitoring

Sevco uses a variety of tools to monitor Service activity for unexpected behaviors. For example, since all AWS activity is logged with CloudTrail, we use GuardDuty to monitor those CloudTrail logs for any of the hundreds of findings natively supported by GuardDuty.

Any notice from any monitoring capability is treated with the same urgency as an availability issue and sent directly to the operations staff on call. These engineers receive security alerts, evaluate and respond appropriately. Any abnormal activity is escalated to Tier II security-specific responders for deeper investigation and response.

## Static Analysis

All Sevco source code is automatically scanned by static analysis tools at the time of commit. Any potentially dangerous artifact identified by the source analysis tools blocks the merge of new code into the main branch until the issue is resolved.

There are currently seven different static analyzers running, categorized by development language.

In addition, there are four other analyzers that focus on third party dependencies and any vulnerabilities in those packages.

## Vulnerability Scans

We protect against the two classes of common vulnerabilities that may introduce security risk in a serverless architecture:

- Misconfigured authorization policies that publicly expose resources that should be private
- Third party software packages that introduce known vulnerabilities

Sevco monitors our public resources using a variety of AWS tools such as Scout Suite, AWS Config and AWS Inspector to ensure the publicly available resources match expectations and notify on any unexpected changes.

In addition, as part of our Secure Development procedures, we scan all third party packages used in our software to notify us of any published issues.

Any newly discovered issue in either category is treated as an urgent operations issue with the same priority as a production service outage.

## Penetration Testing

Sevco conducts an annual 3rd party penetration test of its systems. Any findings are reviewed and remediated based on severity and verified as resolved by the 3rd party.

## Backups and Availability

Sevco is architected as a highly available service. Every resource is deployed in multiple data centers (what AWS calls Availability Zones) to help ensure an outage in any single data center does not impact operations in other data centers.

Storage services follow the same highly available model, with all data replicated across each data center.

Finally, all raw data is stored in a highly durable temporary processing queue. In the event of unexpected catastrophic events, Sevco systems are designed to “replay” the raw incoming data and recreate any lost data.

## Change Control

Sevco’s product operations teams follow “Infrastructure as Code” development principles.

When infrastructure is code, we require that it be checked into a source code repository. Our processes are designed such that 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 is required to go through a manual code review process, which includes automated testing and other checks that are used as a conditional acceptance before review by other members of the team.

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."

Sevco's product operations teams are required to follow the same product security program, including the Secure Development Lifecycle that is used to develop our applications. As a result, we require that 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 are designed to alert on unexpected or unsafe changes to critical configurations. If an unsafe change passes each of these controls and still makes it to production, our processes are designed to trigger 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).

## Denial of Service

Responses to Denial of Service (DoS) attacks are tailored to the type of attack.

Sevco APIs and Portal are hosted in AWS, and AWS maintains responsibility for certain classes of DoS attacks as part of their responsibility for "security of the cloud." AWS uses proprietary techniques to mitigate the risk and reduce the impact of many off-the-shelf Distributed Denial of Service (DDoS) attacks.

Other classes of DoS attacks may be categorized as "security in the cloud" and require Sevco action.

In the event of an attack, Sevco 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

Security procedures in our product development teams are governed by the Sevco Product Security Program. It includes three primary components:


- **Product Risk Management Plan**: Designed as a bottom-up evaluation of the risks to product security, the mitigations in place to reduce risks, and the areas in which we are investing to further reduce risks.
- **Secure Development Lifecycle**: Specifies required activities during software development designed to make sure that security is deliberately considered during planning, development, and release testing.
- **Security Response Center**: Monitoring for and responding to vulnerabilities in our products post-release.

## Product Risk Management Plan

Development and management of the risk management process is a high-level and iterative approach, 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

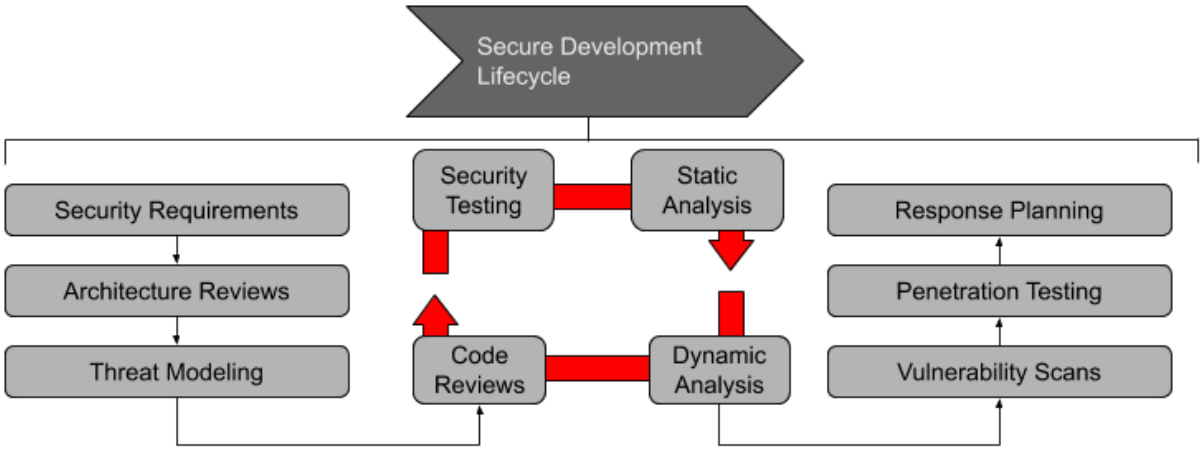
The Risk Management Plan is distinct from threat modeling or architecture reviews. Those activities are part of the Secure Development Lifecycle and apply the business's risk management philosophy to new development. They are executed by the product teams, derived from the guidance in the business's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

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

# Secure Development Lifecycle

Based on industry best practices, Sevco's Secure Development Lifecycle (SVSDL) is designed to identify and mitigate product security risks during the product development phase. It is a collection of activities executed during the development process designed 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 Phase
  - External Vulnerability Scans
  - Penetration Testing
  - Security Response Planning and Coordination




The rigor of our process attempts to prevent vulnerabilities from deployment and is evaluated regularly throughout the year to continue improving the security posture of our Services.

## Security Response Center

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

# Secure Organization

## Policies and Procedures

Sevco maintains a library of information security and privacy policies and procedures. These policies are reviewed at least annually and refreshed as required. They are provided to employees during the hiring process as part of initial training and are available to employees via a web portal.

## Responsibility

The Sevco Security Program is managed through the Security Steering Committee that includes, but is not limited to, the Sevco Chief Executive Officer,  Chief Architect and relevant engineering team leads.

The Committee is responsible for the security program as a whole, including the annual risk management reviews and reviews of organizational security policies.

The CEO is responsible for the day to day execution of business adheres to those procedures.  The Chief Architect manages the day to day execution of the Secure Development Lifecycle and cloud-specific security operations policies and procedures.

## Personnel Security

### Background Checks

Every Sevco employee and contractor undergo background checks before employment begins.  Background checks include SSN Trace, United States-wide criminal database search, sex offender registry search, domestic watchlist search and seven-year county criminal court search.

### Confidentiality Agreements

Every Sevco 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 Employee Code of Conduct

All Sevco employees are bound by the Sevco 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, Sevco 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 Sevco 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 they understand their responsibilities in the security of our systems.

## Data Classification, Data Handling and Data Retention Policies

In addition to the Personnel Security policies that provide guidelines to our employees, Sevco maintains separate policies specific to classification, handling, and data retention. These policies provide guidelines to help ensure consistency across the entire company in the classification, handling, and retention of all data, including customer data.

## Incident Response Plans and Exercises

Sevco maintains a detailed incident response plan to prepare for the technical and administrative aspects of handling a potential breach. Like other policies, the incident response plan is reviewed and updated annually to make sure that it remains consistent and complete.

Each year, the company runs an incident response exercise, where the key participants in incident response from Security Operations, IT, legal, and communications react to potential response scenarios.

Sevco staffs a 24x7x365 team of responders that monitor our Services for suspicious activity, using a variety of data sources and methods. In the event of an actual breach,

we commit to notifying any customer whose data has been compromised as soon as possible.

# Business Continuity Management

## Service Continuity

Sevco's Services are architected to be highly available and minimize or eliminate single points of failure. As described in detail in the preceding section, service architecture follows modern cloud application practices.

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

## Risk Assessment

Sevco's Services undergo an annual risk assessment process that is designed to catalog and quantify risk to the security and availability of Sevco's Services. Any high risk item is considered for additional investment to reduce the risk.

# Privacy and Compliance

## Data Processed

Sevco's Services collect data in four classes:

• **Device inventory and their attributes**: We collect an inventory of your devices from multiple sources and the technical attributes that describe them such as hostname, MAC address, IP address, Operating System and associated users.

• **User inventory and their attributes**: We collect an inventory of the user accounts authorized to access your systems from multiple sources and the attributes that describe them, such as username, first name, last name and user groups.

• **Software inventory and their attributes**: We collect an inventory of the software installed on your systems from multiple sources and the attributes that describe it, such as vendor, product, dependencies and version.

• **Vulnerability inventory and their attributes**: We collect an inventory of vulnerabilities relevant on your systems from multiple sources and the attributes that describe it, such as CVE, CVSS, KEV and associated descriptions..

Sevco uses these 4 primary asset types and their associated attributes to correlate a single source of truth from multiple sources. Then present a single unified inventory, show how attributes have changed over time and enable queries that span the asset types.

The data can include user or device IDs, IP addresses, email addresses and other that may be considered Personally Identifying Information by some privacy regulations.

## Sevco Privacy Program

Sevco respects and is committed to protecting personal data. Our data protection and privacy program reflects current global principles, legal frameworks and standards on processing personal data.

To read Sevco's full privacy statement, see: https://sevcosecurity.com/privacy

# Regulatory Compliance

## General Data Protection Regulation (GDPR )

Processing cybersecurity asset data 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.”*

Sevco’s Services are aimed at providing visibility and insight into asset anomalies, gaps in network or endpoint security software deployment, and other unique indicators that may inform cybersecurity policy gaps. Please consult your privacy advisor for proper classification of the legal basis under the GDPR before deploying Sevco’s services..