SEEQ SAAS MASTER TRUST POLICY

INTRODUCTION

The Seeq Master Trust Policy covers the operations of Seeq in our Software as a Service (SaaS) model. This document outlines at a high level the nature of the Seeq SaaS offering, especially as it pertains to availability, security, and access control. The details of these procedures are outlined and controlled as part of the Seeq SaaS Operations Manual and other Seeq corporate policies.

The topics covered in this document are:

- Architecture
- System Security
- Data Security
- Authentication
- Software and Threat Defense
- Software Updates and Maintenance Windows
- Compliance
- Seeq Global Regions
- Seeq Shared Responsibility Model
- Response to Government Requests

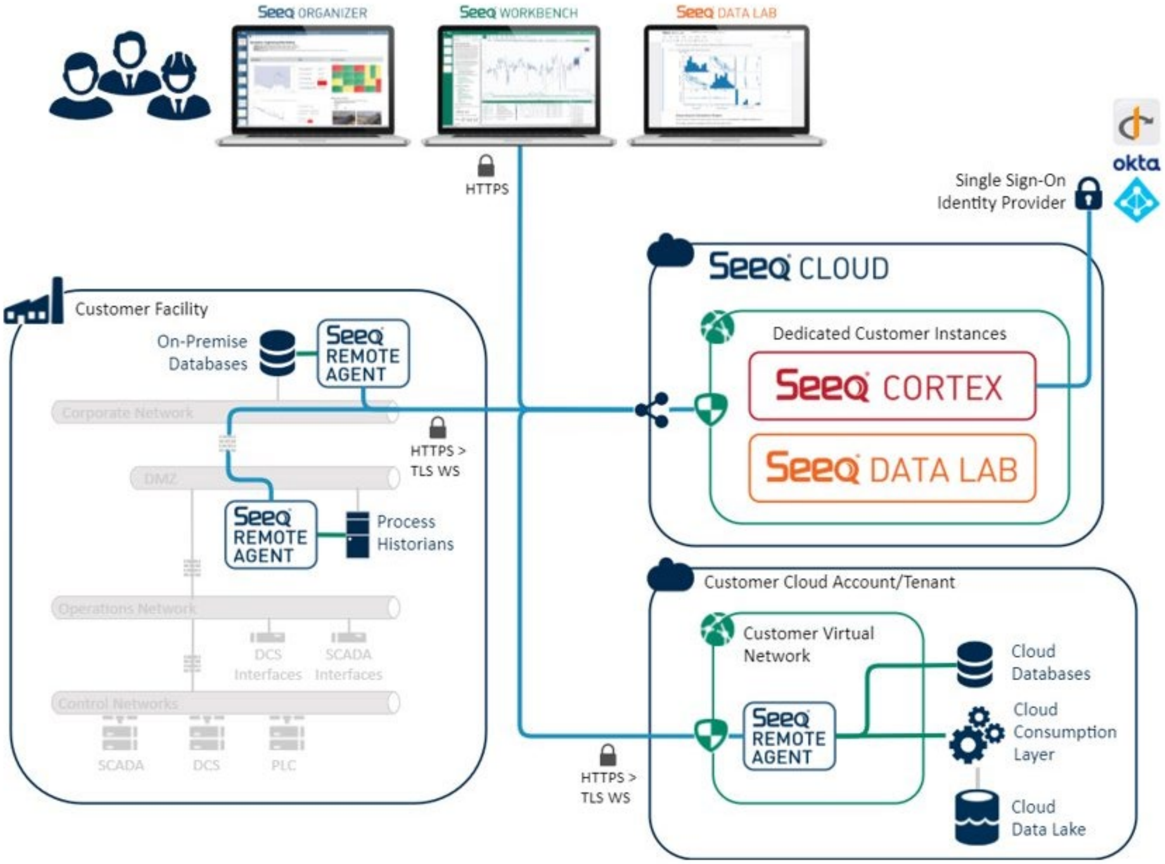
ARCHITECTURE

Seeq SaaS is the primary means of deployment for Seeq in the cloud, utilizing AWS (Amazon Web Services) and Microsoft Azure public cloud providers in conjunction with on-premise or cloud-tenant datasource accessed via Remote Agents running on the customer's corporate network.

The following is a high-level diagram of Seeq SaaS. The overall architecture consists of the following locations:

- The Seeq SaaS cloud infrastructure
- One or more On-Premise locations where you have your data sources, such as PI historians or other systems.
- Your cloud tenant if you have any cloud resident data sources.

Both on-premise and cloud-tenant data sources communicate with Seeq SaaS via authenticated and encrypted WebSocket connections. These links originate at Seeq Remote Agents deployed into each of these locations, and they provide a means to establish communications between your corporate data network and Seeq SaaS without having to open any inbound ports. All connections are secured via HTTPS (Hypertext Transfer Protocol Secure) and initiated as outbound connections.



SYSTEM SECURITY

Seeq is the first application dedicated to process data analytics. Search your data, add context, cleanse, model, find patterns, establish boundaries, monitor assets, collaborate in real time, and interact with time series data like never before.

Seeq SaaS accesses and handles one of your most important assets: your proprietary data. Securing your data and the data you create with Seeq is our top priority. Seeq leverages robust policies, controls, and systems to protect your data.

If you end your subscription, you can take your data with you.

Physical Security

Seeq SaaS is hosted in Azure and AWS cloud infrastructures. In doing so, we inherit all the security best practices of these industry leaders, including physical security of the underlying data centers.

Seeq personnel require administrative access to the infrastructure which delivers Seeq SaaS. Administrators require access to the cloud vendor consoles and to the cloud resources that make up the Seeq Installation. All access is authenticated through Multi-Factor Authentication (MFA).

Access to these systems is limited to the following personnel. All personnel listed below have completed background checks and meet other standards as defined in our corporate policies.

- **Cloud Vendor Administrative Consoles**

  Seeq limits access to the cloud vendor console to the following Seeq roles:

  - Chief Product Officer, VP of Engineering, Chief Architect
  - SaaS Operations Team
  - Technical Support Team

- **Administrative Access to Seeq Installations**

  Seeq is deployed either on discrete Virtual Machines or as a cloud native application utilizing containerized technologies. Systems administrative access to either the virtual machines and/or the deployed containers is limited to the following Seeq roles:

  - Chief Product Officer, VP of Engineering, Chief Architect
  - SaaS Operations Team
  - Technical Support Team

Systems Monitoring

Seeq actively monitors all SaaS deployments to ensure availability. If a service outage is detected, alerts are automatically raised to the SaaS Engineering team, Technical Support team, and are visible to Seeq Management.

Logging and Auditing

Seeq utilizes the auditing and logging features of AWS and Azure to ensure that the infrastructure and security features remain in place, and that changes are only made via approved and reviewed mechanisms as part of our Change Management process.

The Seeq application also maintains a set of logs. These logs are enabled and aggregated to enable troubleshooting by both the technical support team, but also Seeq development engineers assigned to escalated issues. Logs are retained for one year as defined by the Seeq SaaS Operations Manual.

Access to Seeq computer systems is terminated upon the termination of any Seeq personnel.

Open Ports

Seeq accepts only HTTPS traffic and only on port 443. The Seeq authentication gateway is accessible to all IP addresses, but only authenticated traffic can proceed to access the Seeq application.

Access to Seeq SaaS requires only OUTBOUND access from your network to these ports. All connections are initiated from inside the corporate firewall to the Seeq SaaS cloud. This connection consists of a bi-directional WebSocket. This allows Seeq-SaaS to send requests for data to your data sources without the need to open inbound ports on your firewall.

Information Security Incident Response

Seeq will respond to an *information security incident* with a process intended to inform stakeholders of known business impacts and minimize those impacts to the extent possible. Stakeholders can include customers, employees, investors, vendors, and anyone else associated with the company.

This policy is to be applied as soon as information systems or data are suspected to be affected or are evidently affected by an adverse event which is likely to lead to a security incident.

Incident Definition

Seeq has a defined Incident Response Program to address any Information Security Incidents as well as any disruption of system availability. An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Credible attempts to gain unauthorized access to data or systems.
- Changes to data, information or systems without the company's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of a system for the processing or storage of data by any person.

Incident Management Procedure

Events need to be reported at the earliest possible stage by any employee that observes them or when reported by a Service Provider, at the earliest possible stage to the Corporate Information Security Lead (define in matrix below and hereafter referred to in this section as the "lead"), who works with appropriate personnel to identify when a series of events or weaknesses have escalated to become an incident.

When the Lead determines that an incident has occurred, an assessment of the scope of the incident is made and a list of stakeholders is assembled. For example, if a customer's SaaS deployment has been breached by unauthorized parties, the stakeholder list must include the Seeq software administrators within the customer's organization.

The lead works to identify the root cause of the incident and works with appropriate personnel to take corrective action immediately to eliminate the vulnerability. If such action takes longer than 24 hours, the stakeholders must be notified of the incident in advance of the corrective action taking effect. If the corrective action is taken in less than 24 hours, stakeholders can be notified of the incident and the completed action simultaneously. In either case, if stakeholders must take further action, clear instructions must be provided.

An incident is considered closed when corrective action has been taken and stakeholders have been notified.

Information Security Responsibilities

The following table lists the Seeq responsibilities and assignment (lead) on information security:

Responsibility	Responsible Roles
Grant personnel access to Seeq and Customer systems as appropriate to employee role and business needs.	• VP of Engineering or • Chief Product Officer or • Designee acting at the direction of the above
Remove access to Seeq and/or Customer systems upon employment termination or change in job role no longer requiring such access.	• VP of Engineering or • Chief Product Officer or • Designee acting at the direction of the above

Responsibility	Responsible Roles
Approval of sharing of product information beyond current Seeq employees	- VP of Engineering or - Chief Product Officer or - Chief Technology Officer
Management of reported information security events, weaknesses, and incidents	Corporate Information Security Lead
Incident Response Team	VP of Engineering, Support Team Manager, Corporate Information Security Lead, and any personnel involved in the incident

Consequences for Non-Compliance

Training on the Incident Reporting policy is part of Seeq's new-hire and Annual Cyber Security training. Non-compliance with this policy can result in disciplinary action up to and including termination of employment or consulting arrangement.

DATA SECURITY

Data in transit. Seeq employs TLS (Transport Layer Security) 1.3 for secure HTTPS communications. These communications are encrypted between all Seeq user sessions and the Seeq SaaS cloud, as well as all connections between the Seeq Remote Agents and the Seeq SaaS Cloud. In certain cases, Seeq may employ TLS 1.2 for compatibility with older corporate firewalls.

Data at rest. All customer data is encrypted at rest using managed keys.

The storage of customer data is 100% segregated by customer. Seeq does not employ shared databases or filesystems as an approach to multitenancy.

Backups

Seeq automatically performs backups of all data daily. Backups do not disrupt Seeq availability. Seeq retains daily backups for 30 days and retains monthly backups for 1 year. All backups are encrypted at rest using managed keys.

Seeq backups support a Recover Point Objective (RPO) of 24 hours, and a Recovery Time Objective (RTO) of 24 hours.

Seeq uses cloud-vendor native backup systems, which provide exceptionally durable storage (at or above "11 9's" of durability).

The integrity of the Seeq backup system is tested regularly by restoring sample customer backups and reconstituting full Seeq deployments to verify the integrity and utility of the backup. The Seeq Backup Plan is available for review upon request.

Seeq backups are also replicated to a second geographically diverse location to provide Disaster Recovery options. Daily backups are also encrypted and retained for 30 days in the Disaster Recovery location.

Personally Identifiable Information

Seeq collects usage metrics. Seeq uses this data to make the product better and to better support our customers. By default, this data contains usernames and email addresses, but no signal names, values, or other customer data. To comply with any data privacy requirements, customers may choose to anonymize the username and email address through the Configuration tab of the Administration Panel in Workbench.

Personal Identifiable Information (PII) in Seeq is limited to usernames and user emails. Seeq does no processing of PII. Seeq does not transfer PII to third parties without explicit knowledge and approval of the customer. The PII is used exclusively for information security such as authentication and authorization.

Data Disposal

Seeq will dispose of all customer data no later than 3 months after subscription termination or upon written request. Destruction of data by is performed by each cloud vendor and complies with industry best-practices for the non-recoverability of data and decommissioning of media.

AUTHENTICATION

Seeq SaaS can federate with Corporate Identity providers including Windows Authentication, LDAP, Azure Active Directory, Ping Federated, OKTA, and other OIDC-compliant authentication sources. When using these providers, Seeq access is gated by the policies inherent in those providers, ranging from password complexity and rotation to whether Multi-Factor Authentication is employed.

When using certain data sources that maintain user access right via groups, Seeq can support the same item-level security model.

For smaller teams, Seeq also has an internal user database that can be employed to provide user accounts for Seeq. However, MFA (multifactor authentication) is not available when using the internal authentication database.

On-Premise and Cloud-Tenant Data Source Access

Connections to on-premise data sources are made via the Seeq Remote Agent. The remote agent software must run on the customers' network at or near the data source. Authentication to the data source, for example an OSIsoft PI Data Archive, is typically done with a service account local to and authenticated completely within the customer's network. Any credentials needed to access on-premise data sources remain on-premise.

Seeq Application Access by Seeq Personnel

Seeq personnel from either the Analytics Engineering team or the SaaS Operations and Support teams may have a business need to access the Seeq Application deployed for a given customer. This access is limited to those team members and for the scope of time and activity related to performing a specific business function. For the Analytics Engineering team, this could include collaborative use-case development or other contracted activities. For the Operations and Support teams, this access would be to address a specific support case or detected system anomaly.

To provide this access in a secure and managed manner, Seeq SaaS systems need to also integrate with the Seeq Corporate identity provider. Authentication via this system uses strong passwords and Multi-Factor Authentication. This does not provide global access for all Seeq employees.

Access to Seeq SaaS systems is revoked when Seeq personnel have their tenure with Seeq terminated, and/or when an employee's role changes to a function other than those listed in this policy as having a business need for that access.

SOFTWARE SECURITY AND THREAT DEFENSE

Seeq employs a multi-faceted security posture that begins with the design of the software and extends through deployment and post-deployment. This posture includes:

- Annually updated Security Training mandated for all engineers covering topics such as best practices, common vulnerabilities, and recently discovered threat vectors.
- A Security review and Analysis is part of each code change request and is included as part of the mandatory review process for each code change.
- Seeq makes use of third-party vulnerability services to identify and evaluate vulnerabilities for all submitted product installers and container images.
- Seeq subscribes to Security and Threat notification services to receive timely notification of vulnerabilities detected and reported. We have a defined process to assess and evaluate the applicability of these vulnerabilities and create change tickets to implement patches relating to the Seeq product.
- Seeq's SaaS deployment architecture employs industry best practices such as defense in depth, minimizing external threat surface area, isolation of each individual customer data, and minimal permissions for any users or roles.
- Seeq deploys non-customer systems into Seeq SaaS to routinely conduct third-party Penetration testing without risk of exposing customer data.

SOFTWARE UPDATES AND MAINTENANCE WINDOWS

Seeq SaaS will establish a maintenance window on a regular cadence to provide the opportunity to upgrade software and/or apply patches with maximal lead-time and planning for both customers and Seeq. The timing of maintenance window will be established to minimize customer impact, considering time zones and global geography.

The maintenance window will be used, at Seeq's discretion, to:

- Upgrade Seeq Software as needed.
- Patch or upgrade underlying computer systems for performance and/or security reasons.
- Perform infrastructure upgrades as needed to maintain availability and security.
- Perform configuration changes that require a system restart.

If there is no compelling reason to exercise the maintenance window, then Seeq will not interrupt service and defer changes or update to the next maintenance opportunity.

Seeq's policy is to keep Seeq SaaS customer running on up-to-date software running on properly patched systems. This ensures that customers:

- Have access to new and/or improved features in a timely manner.
- Will not experience known defects or bugs for extended periods of time. Issues found-and-fixed for one subset of customers will be made available to the full customer base even before some customers have reason to encounter the issue.
- Receive security patches, both to the components of the Seeq software and the underlying systems, in a timely manner to minimize any threat posed by those vulnerabilities.

Seeq SaaS systems will be upgraded to the latest version of Seeq software within 30 days of the software being released for General Availability. Customers may be upgraded to Limited Availability or Beta releases of software as deemed necessary to provide early access of features to key stakeholder customers or as part of limited availability and/or beta programs.

Seeq retains the final decision as to which version of Seeq software is deployed into Seeq SaaS.

For customers with significant configuration requirements, such as GxP compliance, specific provisions and procedures will be drafted and followed to meet the mutual needs of the customer and Seeq.

COMPLIANCE

Seeq places the highest important on Security and Operational excellence. To that end, we have implemented significant operational controls throughout our organization to establish and maintain compliance with commonly accepted best practices.

Seeq has achieved and maintains SOC 2 Type 2 (Service Organization Control 2) compliance, as validated via external auditors as part of our commitment to Security and Operational excellence. As part of that process Seeq conducts internal audits of our own procedural compliance. We also have an internal process of controls to evaluate and update processes and procedures as dictated by our corporate value of Continuous Improvement. We externally validate our SOC 2 compliance via an annual external audit.

Seeq also has achieved and maintains compliance with the C5 (Cloud Computing Compliance Controls Catalog) standard.

SEEQ GLOBAL REGIONS

Seeq makes use of the global span of our cloud vendors, AWS and Azure, to provide performant and reliable availability on a global basis. Seeq SaaS is available in the **Seeq Americas**, **Seeq Europe**, and **Seeq APAC** regions.

For each Seeq region, there is at least one primary deployment location and a Disaster Recovery location. Daily backups from all Seeq SaaS customers are duplicated to the designated Disaster Recovery location to facilitate business continuity in case of a significant regional disruption.

Seeq can accommodate and comply with customers having specific regulatory or legal Data Residency requirements within the context of this plan, although that may drive the decision as to which cloud vendor Seeq employs.

SEEQ SHARED RESPONSIBILITY MODEL

The efficient, secure, reliable, and effective functioning of Seeq software requires collaborative activities by both Seeq and the customer. In the Seeq Shared Responsibility Model, the various expectations are listed that delineate what activities Seeq can be expected to perform, and which activities are the customer's responsibility.

Operational Capability

Seeq Responsibility	Customer Responsibility
Provision, deploy, and maintain cloud resources sufficient to meet customer needs, both initially and as usage grows, consistent with any contractual limitations and the Seeq Service Level Agreement (SLA).	Provision, deploy and maintain any servers necessary to host Seeq Remote Agent software.
Monitor Seeq SaaS systems for proper performance, making corrections and/or configuration changes as needed.	Allow outbound HTTPS access on TCP port 443 from all remote agents and user workstations to the Seeq SaaS URL.
Perform backups according to the Recovery Point Objectives/Recovery Time Objectives defined in this document. Retain backups for the duration and in the locations described in this document. Perform periodic backup restoration tests to validate the integrity of the backup process.	Provide, maintain, and if necessary, restore, network connectivity from the Remote Agents to the designated URL of the Seeq SaaS using the certificate authorities identified by Seeq to include configuration of necessary firewalls or security devices.
Copy backups to an alternate Disaster Recovery region to facilitate Business Continuity in case of a significant regional disruption.	Supply and maintain any necessary credentials to run Remote Agent services and access data sources.

Security and Compliance

Seeq Responsibility	Customer Responsibility
Deploy and maintain Seeq SaaS and cloud assets in a manner that supports security postures validated through third party audits, such as SOC2.	Patch/upgrade the Operating System of any servers hosting Seeq Remote Agent software, as necessary to insure reliability and security.
Patch/upgrade both Seeq Software and underlying cloud assets to address and respond to evolving security vulnerabilities and threats.	Management of User credentials to include creation, deletion, approving or revoking Seeq access.
Implement and maintain encrypted, authenticated, and efficient network communications means for all communications (User Sessions, Remote Agents, API access) paths to Seeq SaaS.	Provide access to upgrade Seeq Remote Agent software as deemed necessary, either through the Remote Agent Upgrade capability in the Seeq product or manually.
Configure Seeq to authenticate using the Customer's Identity Provider. Manage access by Seeq employees through Seeq Identity Provider.	Provide information necessary to connect Seeq to designated Authentication providers.

Seeq Responsibility	Customer Responsibility
Upgrade Seeq software on a regular and cadence during pre-defined maintenance windows. Patch software and systems as needed to meet security objectives.	

Seeq Product Administration

Seeq Responsibility	Customer Responsibility
Perform operations that are only possible via the Seeq Command Line interface.	Complete Seeq Administrative training and perform administrative functions for Seeq to the degree they are made available via the Seeq Administration User Interface.
Support system configuration and connection of data sources via means defined and to the degree outlined in the customer's support agreement.	Perform initial configuration and connection of data sources with guidance from Seeq. Further configure datasources via the Seeq Administrative User Interface.

RESPONSE TO GOVERNMENT REQUESTS

If a government or law enforcement agency makes a lawful demand for customer data, Seeq will follow these practices:

- Seeq will not supply direct access to customer data unless directed by the customer
- We will always notify the customer of any request unless prohibited by law.
- Seeq will only disclose information when we are legally compelled to do so and only supply the specific data required by the legal order.