Standard Policies and Procedures

Information Security Overview

May 2021

Quinyx AB | info@quinyx.com | www.quinyx.com

Introduction

Purpose

This paper describes integral parts of the Information Security Management System in place to safeguard customer and user data.

Quinyx Security Objectives

Quinyx is ISO 27001 certified which provides evidence that we are constantly improving our processes with a risk based approach to ensure information security is considered in all changes made to the organisation and product.

At Quinyx, we are entrusted to safeguard customer and user data. This is the primary focus of all processes and controls and this is the reason why we continuously evaluate and improve those processes and controls through a risk based approach. Awareness of this focus on information security needs to flow throughout the entire organisation through clear objectives covering risk management, data protection and compliance.

Information Security Management System

Quinyx protects assets through well established and enforced information security policies, steering processes and organisation structure in alignment with industry information security standards. Our ISO 27001 certificate is a proof of our commitment to continuously improve our protective measures to guard customer data.

Risk Assessment

Quinyx performs both periodic and ad hoc risk assessments to avoid impact on information security induced on the services from changes in supporting organisation, documented processes, remediation measures and follow-ups.

Security Architecture

Quinyx services are built using state of the art security best practises, mechanisms and tools to maintain a security architecture, which provides a framework for the standard security controls according to the highest security standards, to prevent unauthorized processing and accidental or unlawful loss, access to or disclosure of customer data.

Follow-up

Quinyx has processes and a supporting organisation in place to ensure that customers are informed of any actual or potential incident that might jeopardise the confidentiality, integrity or availability of customer data.

Certification

Quinyx is certified under ISO 27001, providing proof that our Information Security Management System fulfills the standards to ensure protection of information assets through documented and tested policies, processes, routines and controls for data protection.

Quinyx environments are hosted by AWS (Amazon Web Services), fulfilling ISO 27001 for security requirements, ISO 27017 for cloud security and ISO 27018 for cloud privacy ensuring GDPR compliance.

Quinyx uses independent third parties to perform annual penetration tests, resulting in a report which is shared with customers.

Right to Audit

Quinyx does not allow customers to perform penetration tests or general security audits. Instead Quinyx refers to third party audit reports and certifications mentioned in the section above.

Information Security Officer

Quinyx has an appointed Information Security Officer, with the responsibility to ensure the security of customer data and the fulfilment of the Statement of Applicability stated in the ISO 27001 certificate.

Quinyx AB | info@quinyx.com | www.quinyx.com

Third party management

Third party risk assessments are conducted on a recurring basis to ensure all vendors involved in the processing of customer data complies with Quinyx high security standards.

Protection of Assets

Asset Register

Quinyx maintains an up-to-date register of all assets involved in the processing of customer data including hardware, software, databases and tools, both internal and external.

Protection Against Malware

Quinyx combines a mix of tools, policies and awareness training according to the highest security industry standards to protect the attack surface from being compromised through malware. The specific methods to protect information will differ depending on attack vector and information asset and are customised to safeguard infrastructure, web applications, mobile applications and staff equipment respectively.

Training of Personnel

Quinyx ensures that its personnel, directly or indirectly engaged in providing the offered services, have the requisite security skills and experiences to fulfil their duties, and provides continuous training to maintain adequate security awareness for all personnel.

Quinyx AB | info@quinyx.com | www.quinyx.com

Protection of Customer data

Data Retention

Use of Data

As a supplier of workforce management and workforce optimisation services, Quinyx processes customer data in order to fulfill the obligations under the agreement.

During the time that Quinyx provides its service to a customer, the customers retains rights to its data processed and Quinyx is obliged to:

- not, without prior permission including under applicable agreements, make customer data available or otherwise disclose customer data to unauthorised individuals, entities, or processors.
- only collect and process personal data for the specified, explicit and legitimate purposes under the agreement.
- retain the customer data only as long as permitted under applicable agreements including as long as necessary to fulfil its contractual obligations and the purpose(s) for which it was collected.
- establish and maintain appropriate organisational and technical security measures to protect customer data from loss, misuse, unauthorised access, disclosure, alteration or unauthorised destruction.

Data Maintenance

Quinyx provides APIs and GUIs to facilitate the creation, maintenance, deletion and retrieval of customer data. In the case of termination of contract, Quinyx will agree a time window for data retrieval through APIs for migration purposes before erasing customer data in accordance with applicable agreements.

Data Alteration

Quinyx does not alter any data stored or processed on behalf of the customer unless permitted under applicable agreement or as otherwise instructed to do so.

To the best of Quinyx knowledge, the service does not contain any program code, programming instruction or set of instructions that have been constructed with

the ability to damage, interfere with, disable, adversely affect or otherwise negatively impact customer operations through the use of the services provided by Quinyx.

Data Erasure

Quinyx will, within a mutually agreed time frame, upon termination of the agreement, securely erase all customer personal data hosted in all environments.

Abusive Access

Quinyx will immediately inform the customer of any request for, ordered by or self-executed activity by any government or private organization, whether by themselves or by a party acting for them, for any access to customer data, as permitted by law, which are related to the customer.

Test Data

All personal data and sensitive information not needed for test purposes is removed or modified beyond recognition before restoration in test environments.

Data Access

Access to customer data for Quinyx personnel is traceable, time limited and follows strict approval processes.

All digital work environments are safeguarded with a central authentication mechanism which ensures that users only have access to data in each respective software application that is crucial to their ability to fulfill Quinyx's agreement with the customer.

Master Account/Subscription

Access to customer data is restricted to personnel based upon the principle of least privilege and supported through technical controls. Reasons for data access include initial configuration, support and troubleshooting.

Quinyx provides strong authentication mechanisms in the form of multi factor authentication for privileged access as system manager.

API Authentication

API Security enforces strong policies around the length and complexity of credentials. Customer client (API integrator) credentials are never stored as plain text within Quinyx systems, instead those are hashed using strong hashing techniques - which eliminates the possibility of unauthorized access from internal Quinyx systems.

Quinyx uses dynamic IPs for all externally exposed endpoints, and allows customers to define whitelisted IP ranges for API usage.

End-User Authentication

Quinyx allows the customer to configure the service with the proper level of authentication mechanisms, from built in basic authentication with configurable levels of complexity and enforcement of password change policies, to multiple factor authentication through customer configured SSO integrations.

Secure Hosting

Quinyx services are hosted by AWS, fulfilling ISO 27001 for security requirements, ISO 27017 for cloud security and ISO 27018 for cloud privacy ensuring GDPR compliance. (Read more about AWS hosting environment's physical security and access at: https://aws.amazon.com/compliance/, and specifically AWS Security White PaperPhysical and Environmental Security).

Data Location

Quinyx uses AWS for data hosting and offers the options to the customer to choose between hosting in the EU with Frankfurt as primary site and Ireland as secondary site or in the US with North Virginia as primary site and Oregon as secondary site. Data is only stored, archived and processed within the agreed region and jurisdiction unless otherwise agreed with the customer.

Separation of Data

Customer data is logically separated from other tenants through application logic and rigid access controls which are carefully tested and monitored.

Test Environments

Testing, staging and production environments are separated on different network segments and are not connected in any logical way, ensuring that production data remains isolated and protected at all times. All environments listed are hosted using the same security levels as if it is a production environment.

Backup

Quinyx uses AWS automated backup of all data which means the latest restorable time for a database instance is typically within 5 minutes of the current time. Full automated backups of all customer data is done every 24 hours to multiple data centers. Data is also copied in real-time to a database replica on a secondary site to not lose any data in the unlikely event of a full disaster in both availability zones of the main site. Backups are stored for at least 30 days.

Recovery

Recovery and failovers of the backups are tested daily and a full disaster recovery scenario is tested annually.

Encryption Enforcement

Quinyx utilises AWS managed services (such as KMS) to encrypt all data at rest. Information traveling between external systems and Quinyx APIs is securely communicated through Transport Layer Security protocols (TLS 1.2 or higher is required) and encrypted using strong encryption algorithms.

Data that can be utilized to access customer and user data, such as passwords and keys, are stored in encrypted format

Logging and Monitoring

Quinyx WFM includes an audit log for changes made to all relevant data entities, available to customers representative with the proper access rights.

Application usage is logged on a fine grained level allowing Quinyx technical teams to troubleshoot, monitor and react to automated alerts related to anomalies in performance, usage and traffic.

Quinyx AB | info@quinyx.com | www.quinyx.com

Vulnerability Analysis

Utilising tools offered by AWS allows us to monitor and ensure compliance of the infrastructure including always-on network flow monitoring which inspects incoming traffic to AWS and uses a combination of traffic signatures, anomaly algorithms and other analysis techniques to detect malicious traffic in real-time to ensure availability and DDoS protection.

Patch Management

Quinyx has a progressive upgrade policy where we by default apply patches for all possible CVE's (Common Vulnerabilities and Exposures) as soon as practically possible, where high impact has highest priority. In cases where upgrading immediately isn't possible we analyze the risk and impact of the specific vulnerability and decide whether they pose an actionable attack vector to us or our customers using the services before upgrading. All servers are running Linux operating systems that are hardened to the usage of the specific server.

Secure Change Management

Software Development Lifecycle

All changes to the product follow a well defined change release management process which includes steps and controls for designing, implementing, reviewing, testing and releasing any change. The starting point and core of any change is a risk based assessment to determine the impact on information security, business priorities, technology, user experience and quality. Decisions are traceable through issue tracking tools and code changes are traceable version control tools.

Change Communication

Changes to Information Security Policy

Quinyx does not introduce any changes that in any material way lowers the security level of the service. We communicate all changes to our information security policies well in advance (at least 2 month) of any changes.

Changes to the Service

Quinyx continuously and seamlessly updates infrastructure and applications to enhance the service and increase information security.

Major changes are available for review on a test instance and communicated through release prior to the release. Release of new functionality or replacement of existing functionality are communicated well in advance through the publicly available knowledgebase and through customer success managers.

Incident Handling and Response

Quinyx has tested routines and monitoring mechanisms in place to detect and react promptly to resolve any security incidents compromising the confidentiality, integrity and availability of customer data.

Breach Notification

Quinyx has tested routines and monitoring mechanisms in place to detect data breaches and shall notify the affected customers without undue delay upon discovery of any breach of security or operational fault leading to the destruction, damage, loss, misuse, alteration, unauthorized disclosure of, or access to a user's personal data.

Business Continuity

Business Continuity Planning

Quinyx has a business continuity plan in place with assigned roles and responsibilities to ensure a timely recovery from any unplanned interruptions of operations.

Redundancy

Quinyx SaaS is hosted in at least 2 availability zones per primary region with a secondary region for additional redundancy. This allows us to maintain high

availability and guarantees instantaneous disaster recovery through a fail-tolerant architecture.

Planned Interruption

Quinyx will use reasonable endeavours to notify the customer at least seven (7) days before any scheduled maintenance window. Such notification also includes information about the material changes in the upcoming release.

Compliance

Compliance with Laws

Quinyx will comply with all statutory requirements relating to data protection in all sites where Quinyx is present.