Quester Approach to Security and Compliance

Last Updated: 2/7/2025

Quester

Table of Contents Table of Contents

Quester

Overview

Security, Privacy, Transparency and Compliance are a key focus for us at Quester. This security guide is meant to help our customers and partners understand the security program at Quester. At Quester we are fully committed to protecting the confidentiality, integrity and availability of the data entrusted to us. To uphold this commitment, we have put in place an Information Security Program that follows the guidelines of the NIST Cybersecurity Framework (CSF) 2.0 and SOC2. These frameworks offer a scalable approach to managing and mitigating cybersecurity risks throughout our organization, enabling us to safeguard our assets and adapt to the changing threat landscape.

Our commitment to our clients, partners and employees:

- Treat your data like it is our own.
- Follow all required laws and regulations to protect your data and privacy.
- Never share your confidential data with any external parties without your expressed permission

Quester

Security & Compliance Environment

Governance

Quester's Security & Compliance Committee includes leaders from various teams including its Senior Vice President of Information Technology, Human Resources and security and compliance team. Designees from the committee will meet on a weekly, and monthly basis to review potential risks and remediation activities and discuss ways to improve the security posture of the organization. The committee also briefs the President on the status of Security & Compliance on an annual basis.

Policies & Procedures

Quester has a comprehensive set of security, privacy, and compliance policies and procedures. All policies are reviewed and signed off by the security team on an annual basis. All personnel will attest to the receipt and review of these policies and procedures.

Certifications and Regulatory Compliance

Quester follows the guidelines of the NIST Cybersecurity Framework (CSF) 2.0 and is undergoing its SOC2 - Type II assessment. Quester is also CCPA and GDPR compliant.

Infrastructure & Software

Quester is hosted on Ntirety's infrastructure, which provides a robust set of managed services, including 24x7 phone and ticket support, incident response, availability and capacity monitoring, notifications, managed patching, platform and application expertise, fully managed infrastructure, co-administration of operating systems, and file system backup monitoring and management.

Quester

Vulnerability Management

The Quester vulnerability management program continuously monitors its environment for vulnerabilities. This program includes **monthly** code vulnerability scanning such as finding security issues in the code and hard-coded secrets in the git repos. Ntirety manages security of the cloud environment. Additionally, Quester conducts 3rd party network and application penetration testing, Business Continuity/Disaster Recovery Testing, and Incident Response Testing on an **annual basis**.

The Security team is responsible for prioritizing the vulnerabilities based on the severity and working with various stakeholders towards remediation and mitigation of associated risks.

Continuous Monitoring

Quester's continuous monitoring focuses on the information and alerts gathered from actions performed by the employees on their devices, network traffic and other internal logging. Alerts are triaged and responded to by appropriate stakeholders.

Business Continuity, Disaster Recovery, Incident Management

Quester has formal Business Continuity, Disaster Recovery, and Incident Management plans that govern how to respond to catastrophic events such as an earthquake or pandemic that impacts a region where Quester has operations. These plans are tested at least annually.

Access Control

Quester maintains an inventory of essential information assets and information. Quester adopts the principle of least privilege for all accounts and limits access to confidential data only to personnel who require that access for their role in serving our partners.

Quester maintains separate development, user acceptance testing, and production environments, and access to each environment and within each environment is strictly controlled. All access to Quester's servers or Customer Data is logged and is protected by various controls including strong passwords, multi-factor authentication, and VPN.

Personnel Security

Quester conducts a background investigation of all employees prior to employment. All employees at Quester receive Security Awareness, Privacy and Phishing prevention training and must sign a nondisclosure agreement, the Quester Code of Conduct, and Acceptable Use policy when their employment begins. In addition, all employees are informed of and agree to comply with Quester's security policies and practices as a part of their initial onboarding. System administrators, developers, and other users with privileged usage receive special and ongoing training and are subject to additional background screening.

Physical and Environmental Security

Quester's Physical Security Policy ensures the safety and security of its facilities and information systems by restricting access to authorized personnel only. All employees and contractors must adhere to physical security procedures, including escorted access for visitors and vendors, and report any unauthorized access incidents. A record of all physical access, including visits and maintenance to production and secure environments, is maintained. The policy also covers the protection of off-site equipment and outlines responsibilities for securing physical security equipment, such as locks, walls, doors, and surveillance cameras.

Quester

Encryption

Quester uses industry-accepted encryption standards to protect Customer Data and communications. All sensitive data is encrypted in transit using HTTPS and at rest. Additionally, any communications or file transfers are encrypted using TLS.

Encryption

Quester is hosted on Ntirety's infrastructure, which provides managed services such as 24x7 support, incident response, monitoring, managed patching, and platform expertise. All backups are encrypted and monitored through Pingdom and ScienceLogic Monitoring System, with alerts triggered in case of failure. Quester's data retention policies ensure compliance with regulatory and contractual requirements, safeguarding customer and system data.

Service & Availability

Quester keeps monitoring the uptime of the service. Our infrastructure makes sure to alert the engineers if there is any downtime with any of our services to get immediate attention.