v2023.1

QUID

Security Policy

Last Updated: August 2023
Revision #: Final

QUID CONFIDENTIAL INFORMATION

Table of Contents

SECURITY POLICY

1. Introduction

This document explains the security policies of NetBase Solutions, Inc., d/b/a Quid ("Quid"), pertaining to their cloud-based, SaaS (Software as a Service) applications (collectively, the "Quid Platform Services"). The Quid Platform Services are hosted centrally and licensed on a subscription basis to Our customers, who are allowed to access the Quid Platform Services using a thin client from a web browser. This method provides customers with on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, that can be provisioned and released.

Quid employs state-of-the-art security technologies to facilitate confidentiality, application uptime, and business continuity. We store public data from third party sites, such as social media sites, blogs, and news providers, on behalf and for the benefit of our customers. We also store a small amount of user data (such as names and email addresses of the customer's users), and, in limited cases, Customer Confidential Information. Quid does not accept Personally Identifiable Information (PII) in Customer Confidential Information. Quid supports integration with other systems via APIs, not direct integration.

2. Purpose

Information is a vital asset to Quid and our customers. Information of Quid that is classified as Internal Only (Level 1) or Confidential (Level 2) (collectively, "Non-Public Quid information") and Customer Confidential Information requires protection from unauthorized access, modification, disclosure, and destruction.

3. Policy Scope

This policy covers all employees and contractors (collectively referred to as "Personnel") who have access to or are responsible for maintaining Non-Public Quid Information, and/or Customer Confidential Information on (a) the Quid Platform Services or (b) any system, computing resource, or physical facility controlled by Quid.

4. Roles and Responsibilities

Security Officer: Quid Security Officer is Lei Li, CTO. Additional deputy Security Officers augment the Quid Security team as needed.

Security Team: All Quid Personnel responsible for maintaining security at Quid commensurate with their respective roles and responsibilities. All Quid Personnel receive training and refresher training on Quid Security Policy.

5. Definitions

The security practices of Quid related to the Quid Platform Services substantially conform to the following standards:

"Common Software Vulnerabilities" (CSV) are application defects and errors that are commonly exploited in software. This includes: (i) The CWE/SANS Top 25 Programming Errors – see http://cwe.mitre.org/top25/ and http://www.sans.org/top25-software-errors/;

“Customer Confidential Information” is as defined in customer Agreements.

“Industry Standards” are generally recognized industry standards, best practices, and benchmarks including: (i) National Institute for Standards and Technology – see http://csrc.nist.gov/; (ii) ISO / IEC 27000-series – see http://www.iso27001security.com/

COBIT 5 – http://www.isaca.org/cobit/(iv) Cyber Security Framework – see http://www.nist.gov/cyberframework/(v) Cloud Security Alliance – see https://cloudsecurityalliance.org/.

6. Policy Directives

6.1. Data Center Security

Physical Security (Building and/or Restricted Access)

Quid data centers are configured with access control, with visitor areas marked out separately. Visitors are required to carry an entry pass and be escorted by Quid staff when visiting Quid premises. Quid’s data centers are all in compliance with the requirements for Class A in the GB 50174 Code for Design of Electronic Information System and the T3+ standards in the TIA- 942 Telecommunications Infrastructure Standard for Data Centers, including the following:

- Fire detection and handling: Quid data centers are equipped with fire detection systems using thermal and smoke sensors. The sensors, fitted to the ceiling and floor, would give audible and visual alarms when triggered. Each data center comes with an integrated gas extinguishing system and fire extinguishers. Trainings and drills on how to detect and respond to fires are organized regularly.

- Power: To achieve a 24/7 uninterrupted service, Quid data centers are powered by dual main supplies and redundant power systems. In case of a power failure, redundant battery packs and diesel generators are enabled to power data center devices, thus allowing the data center to run continuously for a certain period of time. Quid utilizes N+1 Power Redundancy.

- Temperature and humidity: Quid data centers are fitted with precision air conditioners to ensure a constant temperature and humidity level, which are electronically monitored. In case of any fluctuation of temperature or humidity outside of the normal range, an alarm is triggered, and actions are taken immediately. All air conditioning units work in hot standby mode. Quid utilizes N+2 Cooling Redundancy.

- Quid data centers and server rooms are equipped with security surveillance systems covering all the areas and passages and staffed with security guards for 24/7 patrol. All the surveillance videos and documents are saved and reviewed by dedicated personnel periodically.

Network Security

The Quid network design utilizes redundant components and connections to facilitate availability and security:

- **Limited public connections.** Quid uses the absolute minimum number of public connections. Machines on the public network have only two open ports—80 and 443. An additional port is open for FTP servers; Quid only utilizes secure FTP.
- **Demilitarized Zone (DMZ)**. Publicly accessible servers are placed on a separate, isolated network segment typically referred to as the DMZ.
- **Packet filtering, firewalls, and control devices.** Firewalls are used to manage and restrict inbound, outbound, and internal network traffic to only the necessary hosts and network resources.
- **Intrusion detection and prevention devices.** Quid employs various tools to detect and eliminate any intrusion into our data centers.

- **Continual monitoring.** The Quid network is monitored constantly by automated and manual means with around-the-clock support.
- **Network security.** The Quid production network is only accessible from the outside through proxy servers. For administration, the only way to access the system is via SSH through a gateway with a pre-shared security key and password though an MFA VPN tunnel. In addition, administrators need to provide a password for each individual machine within the system.
- **Protection for public-facing systems.** Quid limits the number of public-facing interfaces. Quid uses a variety of tools, such as Fail2Ban, OWASP Zed Attack Proxy(ZAP) and Nessus, to actively scan our public systems and ban IPs showing malicious activity.
- **Protection for private systems.** Quid continuously scans the private network to identify and address malicious activity, machines exhibiting unexpected usage patterns, and other issues.
- **Database monitoring/protection against IT infrastructure problems.** Quid uses Nagios, Ganglia, and other tools to monitor system resources internally and externally and generate alerts when resources exceed specified thresholds.
- **Penetration/vulnerability testing.** Quid performs network and application penetration testing of its cloud service infrastructure with every software release (which occurs approximately every three weeks) using OWASP Zed Attack Proxy (ZAP). Quid also uses static code analysis scans to detect possible security patterns and Sonatype Component Lifecycle Management to scan for security issues in third-party dependencies. SAP and several Fortune 500 customers have conducted certified, third-party testing against the Quid application. All issues found were remediated immediately and results were shared with participating parties.
- **Production Isolation.** Production systems are physically and logically isolated from Development and Engineering Systems. Production is located in a different Data Center, and VPCs and Security Groups provide logical isolation.

Operating System Patching and Maintenance

Quid maintains up-to-date operating system patches for all hosted systems that process or store Customer Confidential Information. Quid installs critical- and high-rated patches within 30 days of the vendor’s release of the patch.

Change Control

Quid maintains rigorous change control over its Quid Platform Services Production systems. The following list summarizes Quid change control procedures. The full process is documented internally.

- All changes to Production are made only by DevOps Team members,
- All code deployed to Production, including script and configuration files, must be checked in to Git; and
- All code changes are built from source code checked out from Git. All code deployed to Production must have gone through the Quid review and testing process.

6.2. Production Architecture and Network Design

Encrypted Communication

The Quid Platform Services encrypt all traffic between the user's browser and Quid servers using the Transport Layer Security. Quid Platform Services use TLS 1.3 protocol for encryption. The TLS protocol is an industry-standard method for securing and protecting web communications and client/server communications.

Using the TLS protocol, a TLS-enabled server can authenticate itself to an TLS- enabled client and the client can authenticate itself to the server, thereby establishing an encrypted connection between both machines. This encrypted connection provides "channel security," which has three basic properties:

- Privacy: Encryption is used for all messages after a simple handshake defines a secret key. The initial key exchange is protected by Public Key Encryption.
- Authentication: The server endpoint of the conversation is always authenticated.
- Reliability: The message transport includes a message integrity check.

A TLS connection provides a high degree of confidentiality by requiring that all information sent between a client and server is encrypted by the sending software and decrypted by the receiving software. Any tampering with data sent over an encrypted TLS connection is automatically detected by a mechanism that determines whether data has been altered in transit.

TLS connections for Quid Platform Services are managed by Quid. TLS encryption is validated by the certification authority DigiCert, which issues a digital certificate, or electronic credential, confirming that Quid is the owner of Quid connections and enabling secure communications between client and server.

Customer Confidential Information Encryption

All customer-provided files containing Customer Confidential Information are stored in encrypted form while "at rest" using AES- 256 in Quid's raw document storage system.

6.3. Application and API Security

User Authentication

Quid Platform Services authentication uses license administration to check the validity of customer and user data before provisioning companies, accounts, and users in the Quid Platform Services. Once verified, Quid administrators create users, assign roles to users, and specify passwords using the Quid Administration console. After the administrator enters a user's access credentials, the system emails the user a message containing a link and token for resetting their password. Users can reset their own passwords at any time.

Single Sign-On

The Quid Platform Services support single sign-on using SAML 2.0 (Security Assertion Markup Language) or Quid's built-in authentication.

User Passwords

A user password must conform to the following guidelines:

- Must contain a minimum of eight characters.
- Cannot contain spaces.
- Must contain at least one number, one letter, and one special character, such as a question mark (?) or plus sign (+).

In addition, Quid does the following:

- When the user enters their password, the system masks the password characters to prevent unauthorized parties from being able to observe or subsequently recover them.
- After ten consecutive, unsuccessful logins, the system locks the user out.
- The system requires a user to reenter credentials after a set time of inactivity.
- Quid prohibits the existence of duplicate, active user IDs.
- Administrators can disable a user ID immediately or as of a future date.

Password Encryption

Quid uses coding based on state-of-the-art algorithms for password encryption. User passwords are not stored directly in the authentication database; instead, Quid holds a digest value calculated from the password plus an undisclosed salt value. The digest method is widely considered to be irreversible. The login process calculates the equivalent digest from the submitted password and allows authentication only if the two match. The password submitted during login is immediately discarded.

When the user attempts to access the Quid Platform Services, the application server intercepts the request and displays a login page where the user enters their username and password. After authenticating the user and checking to see if the user has a role that allows them to access the application, the system displays the application’s home page. Users without valid credentials are blocked at the application server level. A user’s role controls what areas of the application they can view and what tasks they can perform.

Application Database Encryption

Data at rest is encrypted utilizing AES-256 in our application database.

Key Management

The Quid Platform Services utilizes Hashicorp Vault for key management. Keys are rotated on a regular basis and vault servers are on dedicated hardware in private VPC and dedicated security group. All access is logged and audited on a continual basis.

Logging

All access, both customer and Personnel, to the Quid Platform Services Production systems are logged. These logs are stored on multiple servers and retained indefinitely.

User Account Administration

Users of the Quid Platform Services are granted system and network access based on business need. Privileges are granted based on the principle of least privilege.

Vulnerability and Threat Scanning and Remediation

Quid conducts static vulnerability scans on the application source code for Quid Platform Services for each major code release. Quid also conducts external testing of the Quid Platform Services for Common Software Vulnerabilities with each major release. These tests are conducted via third-party tools. All high-priority Common Software Vulnerabilities are addressed within eight weeks of discovery and usually much faster.

Software Patch Management

Quid uses an effective patch management system to regularly update operating systems, firewalls, and other applications with security patches and virus definitions.

Application and Network Scan by Customers

Quid permits customers to perform application vulnerability scans and penetration tests of the Quid Platform Services, generally on a non-Production instance, with prior approval and coordination. Quid will remediate any Critical vulnerabilities as soon as a remediation solution is available and High vulnerabilities within 30 days of detection.

6.4 Office and Corporate IT Security

Physical Security

Access to Quid offices is restricted to Quid Personnel and authorized visitors. Access of Quid Personnel is controlled via keycard. Visitors require an escort. Access is logged and monitored. Access to the network equipment room requires additional authorization. Activities in this room are video recorded.

Wireless Security

All wireless networks utilize strong encryption, such as WPA2, and require a pre- shared key for access. Access to services on the network requires further authentication.

Network Security

Only authorized users are allowed access to Quid networks. Positive identification is required to use the system. The identities of all users must be positively identified with user IDs and secure passwords—or by other means that provide equal or greater security—prior to being permitted to use Quid computers and network resources.

Each user ID uniquely identifies a single user. Quid does not permit shared or group user IDs.

All external network connections are protected by firewalls. External access to internal resources requires logging in through a VPN.

Laptop and Mobile Device Security

Laptop security policies	All Quid laptops include the following security features: • A password is required to unlock the computer. • All laptops have encrypted hard drive(s). • All laptops are configured to lock after fifteen minutes of inactivity. • A personal firewall is installed on the laptop and is always active. • Anti-virus software is required to be installed on laptops. Software must have active scanning and be kept up-to-date. • Quid IT can erase laptops remotely in case of theft or loss.

Mobile device security policies	All Personnel accessing Quid email on a mobile phone or tablet are required to do the following (policies are enforced by Quid IT): • Use a PIN to access the device. • Enable encryption for all Quid and Customer Confidential Information. • Enable Quid IT to remove all company-related data and business applications on the device. • Enable Quid IT to reset the manufacturer's default settings on the device if it is lost or stolen.

Data Encryption

All laptops of Personnel that contain Customer Confidential Information have encrypted hard drive(s).

Personnel Passwords

All Personnel passwords for laptop access must meet or exceed the following guidelines:

- Must contain a minimum of eight and a maximum of 15 characters.
- Cannot contain spaces.
- Must contain at least one number, one letter, and one special character, such as a question mark (?) or plus sign (+).

6.5 Business Continuity

Data Center Backup

All user-facing services are redundant, meaning that they are engineered to keep running even if the underlying hardware fails. Quid maintains multiple copies of both user data and social media data:

- **User data.** Quid maintains multiple copies of user data on two database servers that are each automatically replicated and backed up nightly to a different geographic location.
- **Social media data.** Quid maintains multiple copies of both raw and indexed social media data published within the last 51 months. Indices are replicated both onsite at the Production data center and at another geographically distant datacenter.
- **Consistency testing.** Quid continually tests the user information database for consistency and tests off-site backups of this information monthly.

Offsite Storage

Quid maintains multiple copies of all Production data at geographically distributed data centers. Quid's primary DC location is in Ashburn, VA. Our secondary DC is located in Santa Clara, CA.

Disaster Recovery

Quid has developed a disaster recovery plan that outlines steps the organization will follow to facilitate continuity of service in the event of a major disaster. The recovery time objective is 48 hours. For more information on Quid's disaster recovery plan, contact your sales representative or email support@quid.com.

Laptop Backups

All laptops of all Personnel are backed up daily to a geographically distributed cloud backup service.

Force Majeure Policy

Quid business operations are designed so that Personnel can generally work from any location. Personnel do not need to perform their assigned tasks from a Quid office. In the event of a force majeure event such as a pandemic, fire, flood, or extensive power or internet outage, Quid Personnel will be encouraged to work from home or other safe location until the issue has subsided.

6.6 Personnel Security

Security Training

Quid conducts regular security training for all Personnel. Security training is included in new Personnel orientation for all Personnel. In addition, all Personnel with access to Customer Confidential Information are required to attend refresher training at least annually.

Background Checks

Quid conducts background investigations, subject to local legal restrictions, commensurate to the level of security required for each job applicant. It also may conduct reference checks on all Personnel as part of due diligence in the employment process.

Employee and Contractor Agreements

All employees and contractors in the company are required to sign confidentiality agreements as a condition of engagement.

Terminated Personnel

Access to all systems, both production and corporate IT, is disabled immediately when an employee or contractor is terminated.

Destruction of Customer Confidential Information

Quid will return or securely destroy all Confidential Information provided by a customer within thirty (30) days of:

- Termination of services to the respective customer, or
- Receipt of a request to do so from the respective customer

7 Certifications

The hosting providers Quid uses to support the Quid Platform Services meet the strictest industry standards and hold a number of industry certifications. These include ISO 27001, ISO 20000, ISO 22301, ISO 9001, ISO 27017, ISO 27018, CSA Star, SOC1 Type II, SOC2 Type II, SOC3, HIPAA, MPAA, PCI DSS, SEC Rule-17a, and GDPR, as applicable.

8 Incident Handling, Auditing, and Reporting

Security Incident Handling and Reporting

All Security Incidents are logged in Jira. Quid will notify customers of any Security Incident within 72 hours of detection. Quid will promptly take all appropriate corrective actions. “Security

Incident” means the loss, destruction, theft, or the unauthorized access, use, or disclosure of, Customer Confidential Information.

Cooperation

Quid will reasonably cooperate with customers in addressing and remediating a Security Incident.

8 Policy Control, Maintenance, and Changes

This policy will be reviewed and updated at least annually; however, Quid reserves the right to make changes to this policy at any time, and without advance notice, as reasonably needed to respond to technological changes, changes in best practices, and other factors.

9 Appendixes

9.1 Software Development and Lifecycle (SDLC) Processes

Engineering Environment

- **Programming language.** The majority of Quid software is written in Java.
- **Engineering environment.** Quid uses Eclipse, which enforces coding standards and proper object-oriented design methodologies.
- **Configuration management.** Quid uses Git and Maven.
- **Change management.** Quid uses software change management processes that are documented on the internal wiki site. These include a release checklist that outlines the items checked before deploying a release.

Development Process

Quid uses an Agile software development process, which prescribes frequent software releases and best practices, including:

- Design reviews
- Code reviews and constant measurement of code coverage
- Automated testing
- Automated static analysis
- Automated code analysis to identify patterns that indicate defects and security issues
- Continuous and automated builds and integration to ensure that code is compiling and passing unit tests
- Frequent database migration
- Daily development meetings (“SCRUMS”)
- Gorilla testing
- Regression testing
- Data quality testing by in-house linguists and crowd-sourced annotators

Quid maintains documentation on the above procedures on the Quid wiki site. Test cases are stored in the Jira system.

Testing Process

Quid’s Production and Testing environments are isolated from each other. Quid uses a sample of the data index containing publicly available social media data for testing and regularly deploys the application to test servers for automatic testing.

All deployments from Development to Production are performed by the Operations team according to a detailed checklist.

Software Release Process

Quid releases new software roughly every three weeks, typically on Wednesday evenings.
Deployments take between 10 - 30 minutes.

Customers receive notice of major feature enhancements.

Quid occasionally patches the current release to address urgent issues. Most patches do not cause any downtime for customers.

9.2 Internal Vulnerability Assessments of Systems, Applications, and Networks

A summary of Quid’s latest internal vulnerability findings is available to customers on request.

9.3 Third-Party Legal Clauses and Confidentiality

Quid requires all vendors and other third parties who have access to Non-Public Quid Information or Customer Confidential Information to comply with security policies that are at least as strict as Quid’s. The Master Services Agreement governing use of the Quid Platform Services by customers is located online at https://terms.quid.com/msa.