# Table of Contents

1. Introduction ........................................................................................................... 4
2. Purpose ................................................................................................................. 4
3. Policy Scope ........................................................................................................... 4
4. Roles and Responsibilities ......................................................................................... 4
5. Definitions .............................................................................................................. 4
6. Policy Directives ...................................................................................................... 5
   6.1 Data Center Security ......................................................................................... 5
       Physical Security (Building and/or Restricted Access) ........................................ 5
       Network Security ................................................................................................ 5
       Operating System Patching and Maintenance .................................................. 6
       Change Control .................................................................................................. 6
   6.2 Production Architecture and Network Design ..................................................... 7
       Encrypted Communication ................................................................................ 7
       Customer Information Encryption ................................................................... 7
   6.3 Application and API Security ............................................................................. 7
       User Authentication ........................................................................................... 7
       Single Sign-On .................................................................................................... 7
       User Passwords ................................................................................................ 8
       Password Encryption ......................................................................................... 8
       Application Database Encryption ..................................................................... 8
       Key Management ............................................................................................... 8
       Logging .............................................................................................................. 8
       User Account Administration .......................................................................... 8
       Vulnerability and Threat Scanning and Remediation ....................................... 9
       Software Patch Management ........................................................................... 9
       Application and Network Scan by Customers ................................................. 9
   6.4 Office and Corporate IT Security ....................................................................... 9
       Physical Security ............................................................................................... 9
       Wireless Security ............................................................................................... 9
       Network Security .............................................................................................. 9
       Laptop and Mobile Device Security ................................................................. 10
       Data Encryption ................................................................................................. 10
       Passwords ......................................................................................................... 10
   6.5 Business Continuity ......................................................................................... 10
1. Introduction
This document explains NetBase Quid security policies for its cloud-based, SaaS (Software as a Service) applications. The SaaS model hosts applications centrally, licenses software on a subscription basis, and allows customers to access the software 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.

NetBase Quid employs state-of-the-art security technologies to facilitate confidentiality, application uptime, and business continuity. NetBase Quid stores public social media data, a small amount of user data (such as names and email addresses), and, in some cases, customer internal company data. NetBase Quid does not accept Personally Identifiable Information (PII) in customer internal data. NetBase Quid supports integration with other systems via APIs, not direct integration.

2. Purpose
Information is a vital asset to NetBase Quid and our customers. Non-public NetBase Quid and customer information requires protection from unauthorized access, modification, disclosure, and destruction.

3. Policy Scope
This policy covers all personnel who have access to or are responsible for maintaining non-public NetBase Quid or customer information on any system controlled by NetBase Quid, have access to the NetBase Quid network, or store any non-public NetBase Quid or customer information.

4. Roles and Responsibilities
Security Officer: NetBase Quid’s Security Officer is Bob Ciccone, COO. Additional deputy Security Officers augment the NetBase Quid Security team as needed.

Security Team: All NetBase Quid employees and contractors are responsible for maintaining security at NetBase Quid commensurate with their respective roles and responsibilities. All NetBase Quid employees and contractors receive training and refresher training on NetBase Quid’s Security Policy.

5. Definitions

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

6. Policy Directives

6.1 Data Center Security

Physical Security (Building and/or Restricted Access)

NetBase Quid data centers are configured with access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by NetBase Quid staff when visiting NetBase Quid premises. NetBase 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:** NetBase 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, NetBase 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. NetBase Quid utilizes N+1 Power Redundancy.

- **Temperature and humidity:** NetBase 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. NetBase Quid utilizes N+2 Cooling Redundancy.

- **NetBase 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 NetBase Quid network design utilizes redundant components and connections to facilitate availability and security:

- **Limited public connections.** NetBase 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; NetBase 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.** NetBase Quid employs various tools to detect and eliminate any intrusion into our data centers.

• **Continual monitoring.** The NetBase Quid network is monitored constantly by automated and manual means with around-the-clock support.

• **Network security.** The NetBase 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 a MFA VPN tunnel. In addition, administrators need to provide a password for each individual machine within the system.

• **Protection for public-facing systems.** NetBase Quid limits the number of public-facing interfaces. NetBase 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.** NetBase 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.** NetBase 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.** NetBase Quid performs network and application penetration testing of its cloud service infrastructure with every software release (which occur approximately every three weeks) using OWASP Zed Attack Proxy(ZAP). NetBase 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 NetBase 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 differ Data Center, and VPCs and Security Groups provide logical isolation.

Operating System Patching and Maintenance

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

Change Control

NetBase Quid maintains rigorous change control over its Production systems. The following list summarizes NetBase 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.
- All code changes are built from source code checked out from Git. All code deployed to Production must have gone through the NetBase Quid review and testing process.
6.2 Production Architecture and Network Design

Encrypted Communication

NetBase Quid encrypts all traffic between the user’s browser and NetBase Quid servers using the Transport Layer Security (TLS 1.3) protocol. The TLS protocol is an industry-standard method for protecting web communications and ensuring secure 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 NetBase Quid applications are managed by NetBase Quid. TLS encryption is validated by the certification authority DigiCert, which issues a digital certificate, or electronic credential, confirming that NetBase Quid is the owner of NetBase Quid connections and enabling secure communications between client and server.

Customer Information Encryption

All customer-provided files are stored in encrypted form while “at rest” using AES-256 in NetBase Quid’s raw document storage system.

6.3 Application and API Security

User Authentication

NetBase Quid authentication uses license administration to check the validity of customer and user data before provisioning companies, accounts, and users in the NetBase Quid system. Once verified, NetBase Quid administrators create users, assign roles to users, and specify passwords using the NetBase 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

NetBase Quid supports single sign-on using SAML 2.0 (Security Assertion Markup Language) or NetBase Quid’s built-in authentication.
User Passwords
A 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, NetBase 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.
- NetBase Quid prohibits the existence of duplicate, active user IDs.
- Administrators can disable a user ID immediately or as of a future date.

Password Encryption
NetBase Quid uses coding based on state-of-the-art algorithms for password encryption. User passwords are not stored directly in the authentication database; instead, NetBase 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 NetBase Quid application, the application server intercepts the request and displays a login page where the user enters their user name 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
NetBase Quid utilizes Hashicorp Vault for key management. Keys are rotated on yearly basis and vault servers are on dedicated hardware in private VPC and dedicated security group. All access is logged and audited on continual basis.

Logging
All access, both customer and employee, to NetBase Quid Production systems are logged. These logs are stored on multiple servers and retained indefinitely.

User Account Administration
NetBase Quid users 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**

NetBase Quid conducts static vulnerability scans on the application source code for each major code release. NetBase Quid also conducts external testing of the application(s) 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**

NetBase Quid uses an effective patch management system that ensures that operating systems, firewalls, and other applications are regularly updated with security patches and virus definitions.

**Application and Network Scan by Customers**

NetBase Quid permits customers to perform application vulnerability scans and penetration tests of the NetBase Quid application, generally on a non-Production instance, with prior approval and coordination. NetBase Quid will remediate any critical- and/or high-rated vulnerabilities within eight weeks of detection.

### 6.4 Office and Corporate IT Security

**Physical Security**

Access to NetBase Quid offices is restricted to employees, contractors, and authorized visitors. Employee and contractor access 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 NetBase 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 NetBase Quid computers and network resources.

Each user ID uniquely identifies a single user. NetBase 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

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

<table>
<thead>
<tr>
<th>Mobile device security policies</th>
<th>All employees accessing NetBase Quid email on a mobile phone or tablet are required to do the following (policies are enforced by NetBase IT):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Use a PIN to access the device.</td>
</tr>
<tr>
<td></td>
<td>• Enable encryption for all NetBase Quid and customer data.</td>
</tr>
<tr>
<td></td>
<td>• Enable NetBase Quid IT to remove all company-related data and business applications on the device.</td>
</tr>
<tr>
<td></td>
<td>• Enable NetBase Quid IT to reset the manufacturer’s default settings on the device if it is lost or stolen.</td>
</tr>
</tbody>
</table>

Data Encryption

All employee laptops that contain customer data have encrypted hard drive(s). Any customer data stored on removable media must be encrypted.

Passwords

All 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—they keep running even if the underlying hardware fails. NetBase Quid maintains multiple copies of both user data and social media data:

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

**Offsite Storage**

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

**Disaster Recovery**

NetBase 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 NetBase Quid's disaster recovery plan, contact your sales representative or email support@NetBase.com.

**Laptop Backups**

All employee laptops are backed up daily to a geographically distributed cloud backup service.

**Pandemic Policy**

NetBase Quid business operations are designed so that employees can generally work from any location. Employees do not need to perform their assigned tasks from a NetBase Quid office. In the event of a pandemic, NetBase Quid employees will be encouraged to work from home or other safe location until the danger has subsided.

### 6.6 Employee Security

**Security Training**

NetBase Quid conducts regular security training for employees and contractors. Security training is included in new employee orientation for all employees. In addition, all employees and contractors with access to customer data are required to attend refresher training at least annually.

**Background Checks**

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

**Employee Agreements**

All personnel in the company are required to sign confidentiality agreements as a condition of employment.

**Terminated Employees**

Access to all systems, both production and corporate IT, is disabled immediately when an employee is terminated.
6.7 Destruction of Customer Information

NetBase Quid will return or securely destroy all information provided by a customer within 30 days of:

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

7. Certifications

NetBase Quid’s hosting service meets the strictest industry standards and holds 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.

8. Incident Handling, Auditing, and Reporting

8.1 Security Incident Handling and Reporting

All security incidents are logged in Jira. NetBase Quid notifies the customer of any suspected or actual unauthorized access or sharing of Customer Confidential Information within 24 hours of detecting the incident. NetBase Quid will promptly take all appropriate corrective actions.

8.2 Cooperation

NetBase Quid will reasonably cooperate with customers in addressing and remediating any security incident.

9. Policy Control, Maintenance, and Changes

This policy will be reviewed and updated at least annually; however, NetBase 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. Material changes to this policy will be communicated via online alerts to all current NetBase Quid customers.

10. Appendixes

10.1 Software Development and Lifecycle (SDLC) Processes

Engineering Environment

- **Programming language.** The majority of NetBase Quid software is written in Java.
• **Engineering environment.** NetBase Quid uses Eclipse, which enforces coding standards and proper object-oriented design methodologies.

• **Configuration management.** NetBase Quid uses Git and Maven.

• **Change management.** NetBase 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**

NetBase 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

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

**Testing Process**

NetBase Quid’s Production and Testing environments are isolated from each other. NetBase 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**

NetBase 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.

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

10.2 Topics Covered in the Security Training Program

- Introduction
- Security awareness
- NetBase Quid security policy
- Employee agreements
- Protecting customer information
- Password security
- Physical security
- Social engineering
- Mobile devices and wireless
- Browsing
- Rapid remediation for hacks
- Privacy
- International travel
- Conclusion

10.3 Internal Vulnerability Assessments of Systems, Applications, and Networks

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

10.4 Third-Party Legal Clauses and Confidentiality

NetBase Quid requires all vendors and other third parties who have access to confidential information to comply with security policies that are at least as strict as NetBase’s. Copies of NetBase Quid's standard legal agreements are available on request.

10.5 Privacy Policy