Introduction

Qualia is a settlement software company based in San Francisco that brings efficiency and insight to your title and escrow process, offering full settlement, document preparation, accounting, and title production capabilities. Qualia is committed to protecting our customer's security using the most advanced technology and highest standards. Security has been a core value of Qualia since the inception of the company, and it is our commitment to customer trust which helps shape the decisions that every employee makes every day. This document is intended to provide an introduction to Qualia’s approach to security and how we help our customers maintain the confidentiality, integrity and availability of their data.

Security of Qualia

Qualia's service has been architected to meet the most stringent security requirements of our customers. Security and trust start with transparency, so the following sections present the full stack approach Qualia has taken to protecting them.

DATA CENTER & PHYSICAL SECURITY

Qualia utilizes ISO 27001 and SOC 2 certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS data centers also include several additional environmental safeguards, such as:

- Fire detection and suppression
- Universal power supply
- Climate and temperature controls
- Operational management of systems

For more information about AWS security, please see: https://aws.amazon.com/security.

INFRASTRUCTURE AND NETWORK SECURITY

- **Customer Isolation.** Each individual Qualia customer is provisioned into their own virtualized instance of the service which provides our customers with logical separation of services and data isolation. Typically, in order to scale, cloud providers will use shared infrastructure which commingles customer data Our approach provides Qualia customers with a higher degree of security, privacy, and availability.
• **Data Encryption.** All data transmitted to the Qualia service is encrypted over a secure channel using SSL. Only strong SSL cipher suites have been enabled and further transport layer security, such as Perfect Forward Secrecy, have been implemented.

• **Firewalls.** Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied, and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system’s function. Security groups restrict access to only the ports and protocols required for a system’s specific function to mitigate risk.

• **Spoofing and Sniffing Protections.** Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface to which it is not addressed.

• **Port Scanning.** Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

• **Hardened Hosts.** Qualia infrastructure is proactively locked down, disabling unnecessary ports, services, and users to reduce our attack surface. Hosts are promptly patched and upgraded when security updates are available. Each host runs anti-virus, for which signatures are updated daily.

• **Configuration Scanning and History.** The Qualia infrastructure is continuously scanned for configuration changes outside of its secure baseline. Any change outside of its standard is immediately alerted and mitigated as appropriate. A full configuration history and inventory of Qualia’s infrastructure is maintained for posterity and forensics.

**APPLICATION SECURITY**

• **Secure Design & Frameworks.** During all feature design and development, security is taken into account. As new features are developed they are reviewed for potential security issues, which are then remediated prior to release to production. Security frameworks have been built to mitigate the most common types of software vulnerabilities to enable secure-by-default development practices. Security staff and development teams continuously keep abreast of new threats as they arise.

• **Security Testing.** Qualia undergoes penetration tests, vulnerability assessments, and source code reviews to assess the security of our application, architecture, and implementation. Internal and third party security assessments cover all areas of our platform including testing for OWASP Top 10 web application vulnerabilities and customer isolation. Qualia works closely with external security experts to review the security of the platform and applications and to apply best practices.

• **Vulnerability Disclosure.** Qualia highly values the work of independent security researchers. We support a responsible disclosure policy and will partner with researchers to address security concerns identified in our service in a timely manner. Reports of potential security issues can be sent to security@qualia.com.

**LOGGING, MONITORING AND RESPONSE**

Every individual service component in Qualia logs activity and security events to a centralized logging service which is actively monitored by our engineering staff. Security logs are kept for at least one year. Identified incidents are treated with the utmost priority and are worked on 24/7 until resolution.
AVAILABILITY AND DISASTER RECOVERY

Qualia employs strong platform-level isolation which enables increased service availability. All customer data is actively backed up into secure containers in case of system failures beyond our control.

SERVICE OPERATIONS

Qualia staff does not access or interact with customer data or applications as part of normal operations. There may be cases where Qualia is requested to interact with customer data or applications at the request of the customer for support purposes or where required by law. Access to this data is logged and only named individuals in specific roles are allowed access.

All new Qualia employees go through a thorough background check as part of the on-boarding process. Separate testing and production systems are maintained. Per policy, customer data is only stored within the production service.

PRIVACY

Qualia’s privacy policy is documented in our Platform Agreement and clearly defines what data is collected and how it can be used. Qualia is committed to customer privacy and transparency.

We take rigorous steps to protect the privacy of our customers and protect data stored within our platform. Some of the protections inherent to Qualia’s product include authentication, access controls, and data transport encryption. Security protections of the platform are described in detail throughout this white paper.

COMPLIANCE

Qualia is built upon infrastructure which is ISO 27001 and SOC2 compliant. Internal security policies are built around the ISO 27001 information security framework and we routinely audit our security and compliance posture through automation and manual assessments. Qualia is built to enable our customers to more easily adhere to ALTA best practice pillar number 3 (information security and privacy) by helping remove some of the large overhead required to securely manage your customer’s data with the highest level of security.

SECURITY FEATURES OF QUALIA

Administrative controls and security features of Qualia, such as multi-factor authentication, are described in detail in Qualia’s product documentation, located at https://qualialabs.zendesk.com.