QUALIFIED

Trust is our #1 value.

Every day we try to earn your trust in our security practices and operations.

Overview

The security and integrity of customer data is paramount to our customers' values and operations. That's why we've made Customer Trust our number 1 value at Qualified. The landscape of Information security and data privacy law, standards, and compliance requirements are constantly changing. It's important that companies are transparent about how they are addressing this ever-changing landscape. Qualified helps customers maintain control of their privacy and data security in a myriad of ways:

Data Security: We provide our customers compliance with high security standards, such as encryption of data in motion over public networks, auditing standards (SOC 2), Distributed Denial of Service ("DDoS") mitigations, and dedicated support and success services.

Disclosure of Customer Service Data: Qualified only discloses Service Data to third parties where disclosure is necessary to provide the services or as required to respond to lawful requests from public authorities.

Trust: Qualified has developed security protections and control processes to help our customers ensure a secure environment for their information. Independent third-party experts have confirmed Qualified's adherence to high industry standards.

Access Management: Qualified provides an advanced set of access and encryption features to help customers effectively protect their information. We do not access or use customer content for any purpose other than providing, maintaining and improving the Qualified services and as otherwise required by law.

Customers and Partners

- Privacy Policy
- Terms of Service
- Data Processing Agreement

Compliance and Certification

GDPR

Qualified is fully committed to compliance with the GDPR. Our dedicated GDPR page provides a high level summary of our commitment. Please contact us at privacy@qualified.com directly with any questions as it relates to our commitment to data privacy and protection relating to the Qualified service.

Privacy Shield

Qualified has certified its compliance with the EU-US Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.

For more information about the Privacy Shield, see the US Department of Commerce's Privacy Shield website located at: https://www.privacyshield.gov. To review our certification on the Privacy Shield list, see the US Department of Commerce's Privacy Shield self-certification list located at: https://www.privacyshield.gov/list and search for "Qualified.com".

On July 16, 2020, the European Union Court of Justice (CJEU) invalidated the EU-US Privacy Shield in its decision in Facebook Ireland v. Schrems (Schrems II). The court determined that the Privacy Shield transfer mechanism does not comply with the level of protection required under EU law.

Qualified now leverages the Standard Contractual Clauses (SCCs) for data transfers of personal data into the U.S. This includes a Data Processing Agreement for Qualified and all of our sub-processors.

CCPA

Qualified customers that collect and store personal information in Qualified Services may be considered "Businesses" under the CCPA. Businesses bear the primary responsibility for ensuring that their processing of personal data is compliant with relevant data protection law, including the CCPA. Qualified acts as a "Service Provider," as such term is defined in the current version of the CCPA, with respect to the processing of personal information through our Services. Therefore, Qualified collects, accesses, maintains, uses, processes and transfers the personal information of our customers and our customer's end-users processed through the Services solely for the purpose of performing our obligations under our existing contract(s) with our customers; and, for no commercial purpose other than the performance of such obligations and improvement of the Services we provide.

We do not "sell" our customer's personal information as currently defined under the CCPA, meaning that we also do not rent, disclose, release, transfer, make available or otherwise communicate that personal information to a third party for monetary or other valuable consideration. We may share aggregated and/or anonymized information regarding use of the Service(s)—which is not considered personal information under the CCPA.

If you would like to review how the CCPA applies to Qualified's Processing of Personal Data in detail, please click here and see Annex 2 (California Annex)

SOC-2 Type II Report

Qualified has received its SOC 2 Type II compliance certification. Contact your Qualified Representative to request access to the report.

Policies and Procedures

Established Policies

Qualified's policies are managed and updated on an ongoing basis. These policies are reviewed at least annually and compliance with them is considered in each third party audit. The policies include:

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Change Management Policy
- Cryptography Policy
- Data Classification Policy
- Data Deletion Policy
- Data Protection Policy
- Disaster Recovery Plan
- Incident Response Plan
- Passwords Policy
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- System Access Control Policy
- Vendor Management Policy
- Vulnerability Management Policy

A selection of these policies are detailed below. All additional policies are available to Qualified prospective and existing customers under a signed non-disclosure agreement.

Contingency Planning

Qualified Application Availability

The Qualified service infrastructure has been designed to handle outages or failures gracefully. This infrastructure is monitored continually and managed to handle times of increased loads. Any planned outages are communicated to impacted customers well in advance and done so at times of least-impact.

Qualified availability may be found and tracked at status.qualified.com

Business Continuity

- Qualified performs testing of this Business Continuity Plan on an annual basis. The CTO is responsible for coordinating and conducting an annual rehearsal of this Business Continuity Plan.
- Whenever the BCP is enacted, it must be followed up with a retrospective in order to identify lessons learned and playbooks needing creation.
- Business Impact Assessments (BIA's) and Risk Assessments are to be conducted upon onboarding new, business-critical vendors. These Assessments are revisited when the relationship with the vendor changes significantly, including contract renewals. All vendors are required to be reassessed annually.

Disaster Recovery

- Qualified performs testing of the Disaster Recovery Plan semi-annually. The CTO is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan semi-annually.
- Whenever the DRP is used, it must be followed by a retrospective and tabletop reenactment in order to identify lessons learned and playbooks needing creation.
- This policy and plan must be updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and reenactment of past disaster incidents.

Risk Assessment

Qualified is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realized.

Qualified has the primary duty to ensure the Security and Availability of critical systems and customer data. A duty to ensure a secure, available infrastructure requires Qualified to identify and manage risks.

Qualified believes that effective risk management involves:

1. A commitment to the Security and Availability of Qualified infrastructure and services from senior management;
2. The involvement, cooperation and insight of all Qualified staff;
3. A commitment to initiating risk assessments, starting with discovery and identification of risks;
4. A commitment to the thorough analysis of identified risks;
5. A commitment to a strategy for treatment of identified risks;
6. A commitment to communicate all identified risks to the company;
7. A commitment to encourage the reporting of risks and threat vectors from all Qualified staff.

Qualified believes that the following events can trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product or business practices;
2. A significant amount of time (e.g. a year) having passed since the last risk assessment.

Risk assessments can be conducted by unbiased and qualified parties such as security consultancies or Qualified internal staff.

Background Checks

Qualified conducts background checks for all new hires including verification on the following:

- Identity verification
- County Criminal Records Check
- Federal Criminal Records Check
- National Criminal Records Check
- Sex Offender Registry Check
- Global Watchlist Check

Security Training

Qualified employees are required to attend classes upon hiring that cover phishing, password management, physical security and internal-specific matters. They are required to take annual security training following that. Engineers are required to attend an additional technical security workshop. Any changes affecting the product or policies are communicated to Qualified employees and incorporated to onboarding training.

Responsible Disclosure Policy

Vulnerability Disclosures

If you believe you've discovered a potential vulnerability, please let us know by emailing us at security@qualified.com. We will acknowledge your email within five business days.

Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within ten business days of disclosure.

Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of Qualified employees or contractors
- Any attacks against Qualified's physical property or data centers

Thank you for helping to keep Qualified and our users safe!

Data Security and Privacy

Qualified follows all industry best practices to transmit and store data used in Qualified Service Delivery. Below is an outline of these practices.

Data Storage

All data stored by Qualified is done so in a securely encrypted and logically segregated manner. This ensures that our Customers' visitor data is protected from exploitation and accessible for customer support related inquiries. Qualified does not engage in "roll-your-own" encryption, algorithms, or practices and will not use "security through obscurity" within production infrastructure or applications.

Qualified leverages best-in-class cloud-based storage facilities via Third Party Service Providers. to ensure that they have secure physical controls as well as redundant backups to fulfill Business Continuity and Disaster Recovery Plans.
Qualified stores it's data with Salesforce Heroku, who manages cloud servers and databases on AWS. Qualified data resides in the US-East region of AWS, located in Northern Virginia, USA.

Data Encryption

Encryption In Transit

By default all communications from your end users and your visitors with the Qualified Service are encrypted using industry-standard communication encryption technology. Qualified currently uses Transport Layer Security (TLS), with regular updates to ciphersuites and configurations.

Encryption At Rest

All Qualified data is encrypted at rest with AES-256, block-level storage encryption.

Data Retention

We retain Customer Data for as long as necessary to fulfill the purposes set forth in the Qualified Privacy Policy or as long as we are legally required or permitted to do so.

For example, we retain our Customers' account information for as long as their accounts are active and a reasonable period thereafter in case a Customer decides to re-activate our Services; we also retain Customer Data as necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements, and to continue to develop and improve our Services. Customer Data may persist in copies made for backup and business continuity purposes for additional time.

We retain Service Data consistent with our contractual obligations to our Customers.

If you are an end user of one of our Customer's websites, applications, or services, you should review that Customer's privacy policy to learn more about that Customer's privacy practices, including its collection and use of your data, its legal bases for processing your data, and its data retention policies.

Data Deletion

Handling Deletion Requests

By default, a customer's data is stored for the duration of the contract term with Qualified. Qualified provides the option for customers to delete data after their subscription ends. This request must be made by the customer.

Additionally, Qualified provides the option to delete data for individual visitors in compliance with GDPR. This request must be made by the visitor or the Qualified customer. Qualified may require additional ID verification. Qualified will hard delete all information from currently-running production systems within one quarter of the deletion request.Only the authorized employees can delete data in the event that Qualified is requested or required to do so.

Infrastructure and Network Security

Physical Access Control

Qualified is hosted on Salesforce Heroku. Heroku's physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

More information on Salesforce Heroku Security may be found here.
Qualified.com employees do not have physical access to Heroku data centers, servers, network equipment, or storage.

Logical Access Control

Qualified is the assigned administrator of its infrastructure on the Salesforce Heroku Platform. Only authorized Qualified operations team members have access to configure the infrastructure. Each Qualified employee, contractor, and associate has limited access to Qualified systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis.

Penetration Testing

Qualified undergoes black box penetration testing conducted by an independent, third-party agency, on a semi-annual basis. For black-box testing, Qualified provides the agency with an isolated clone of Qualified.com and a high-level diagram of application architecture.

Information about any security vulnerabilities successfully exploited through penetration testing is used to set mitigation and remediation priorities. Qualified will provide a summary of penetration test findings upon request to Enterprise customers.

Third-Party Audit

Third party security testing of the Qualified application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team. Qualified undergoes regular third-party independent audits on a regular basis and can provide SOC-2 compliance audit summaries upon request.

Physical Security

All data center physical security is managed by Salesforce Heroku and Amazon. Heroku utilizes ISO 27001 and FISMA 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.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

For additional information see: https://aws.amazon.com/security

Intrusion Detection and Prevention

Qualified uses an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the corporate headquarters network. Our critical cloud vendors (Salesforce Heroku, Amazon Web Services) also employ sophisticated intrusion detection and deterrent systems. The production servers hosting the Qualified service use a variety of security monitoring tools. Notifications from these tools are sent to the Qualified Security Team so that they can take appropriate action.

Application Security

Single Sign-On

To facilitate user authentication through the web browser and improve identity management, Qualified offers assertion markup language (SAML)-based SSO as a standard feature to customers on its Enterprise plan. SAML 2.0 enhances user-based security and streamlines signup and login from trusted portals to enhance user experience, access management, and auditability.

Qualified integrates with multiple Identity Providers (IdP)—including Okta, Azure, and OneLogin. Using a different IDP? Contact us to find out how we might work with yours.

Software Development Lifecycle

Qualified practices continuous delivery to deliver updates to the Qualified application and infrastructure. All code changes are committed, tested, shipped, and iterated on by Qualified engineers on a high frequency cadence, up to multiple times a day. This allows Qualified to deploy new features, make improvements to existing functionality, and address fixes rapidly.

All of Qualified software is version controlled and synced between contributors (developers) to a single origin repository. Access to the central repository is restricted based on an employee's role. Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.