Qualtrics

Security White Paper Lite

Defining our security processes

Revised February 23, 2015

Version 4.02 • Prepared for External Distribution

www.qualtrics.com/security-statement

Terms & Conditions

This document contains basic information about Qualtrics operations and security. It supersedes all previous versions. While the Qualtrics security team has strived to create an accurate document, Qualtrics does not warrant that this document is error free.

Certain details may have been purposely minimized to protect our intellectual property (IP) rights.

Table of Contents

Executive Summary

If you read nothing else…

This white paper is intended to give the reader an overview of Qualtrics security processes and procedures. It describes key security-related processes performed in all areas of the company, and addresses the security measures we've taken to protect each of those processes (such as secure data collection and disaster recovery).

The key differentiator of Qualtrics and many other SaaS research companies is this: Customers own and control their data and users. Qualtrics treats all customer data as highly confidential, and does not attest or represent the data. In other words, we don't know what data are being collected, and customers are free to use the services as they wish. We use industry best practices to keep data safe from criminals and hackers, and have devised proprietary methods to prevent disclosing data to the wrong requester due to programming errors.

Introduction

WHAT IS QUALTRICS?

Qualtrics is an Application Service Provider (ASP) with a Software-as-a-Service (SaaS) platform for creating and distributing online surveys and related research services. The platform records response data, performs analysis, and reports on the data. All services are online and require no download software; only modern JavaScript-enabled browsers are required (no Java/JVM or Flash). Qualtrics offers three products for online data collection: Qualtrics Research Suite, Qualtrics 360 (Employee Engagement), and Qualtrics Site Intercept. Surveys are usually taken online within a web browser, however SMS surveys are also available.

OVERVIEW OF OUR DATA SECURITY

Qualtrics' most important concerns are the protection and reliability of customer data. Our servers are protected by high-end firewall systems, and vulnerability scans are performed regularly. All services have quick failover points with redundant hardware, and complete encrypted backups are performed nightly.

Qualtrics uses Transport Layer Security (TLS) encryption for all transmitted Internet data. Customers may opt to password-protect their surveys, or have unique ID links that are difficult to guess. Our services are hosted by trusted third party data centers that are SSAE-16 SOC 1 Type 2 attested. All data at rest are encrypted, and data on deprecated hard drives are destroyed by U.S. DOD methods and delivered to a third-party data destruction service.

Security within the Qualtrics Services

All Qualtrics products enable customers to control individual permissions of their accounts and surveys. In other words, Brand Administrators decide who creates, distributes, and analyzes their surveys. There is also an option to prevent surveys from being sent without an approval from a user defined in the workflow.

Our service level standards

Qualtrics serves thousands of worldwide businesses, universities, and other organizations. As a result, Qualtrics must maintain the highest service levels and create environments to minimize downtime. Since 2010, Qualtrics has maintained average up-time of 99.97%.

Disaster recovery plan

Within the continental U.S., Qualtrics maintains production servers in geographically and geologically distinct areas. Qualtrics is prepared to quickly shift to unaffected servers in the event of any local catastrophe.

Our commitment to data security

Keeping customer data secure is of paramount importance. Many of our customers demand the highest levels of data security, and have tested our systems to ensure it meets their standards. In each case, we have surpassed expectations and received high praise from top companies. All Qualtrics accounts are password protected, and all data are replicated in real-time. Passwords are salted, then hashed and stored, making them unknown to any Qualtrics employee. Qualtrics IDs may be linked to the customer's single sign-on services.

WHO OWNS THE DATA IN QUALTRICS SERVICES?

Customers own and control all data entered in or collected by Qualtrics Services. This includes survey definitions, response data, panel data, uploaded content such as graphics, user information, and report results/analysis from such data. Qualtrics may collect anonymous usage statistics (such as number of responses collected) for analyzing performance and calculating account quotas.

Qualtrics only uses customer data to perform the functions required in the Service (such as creating reports). No customer data are ever shared or distributed. And since Qualtrics products are self-service, data are essentially invisible to our staff; customers operate on their own accord.

DATA CLASSIFICATION/REPRESENTATION

Qualtrics does not represent or attest to data entered into its Services since 1) all data and account users are controlled by the customer, and 2) it does not know what data are being stored. Therefore, Qualtrics cannot classify data; it processes all data the same using industry best security measures designed to prevent unauthorized access and disclosure.

ASSESSMENTS AND TESTING

Automated vulnerability scans are performed regularly with a commercial security provider. Complete penetration tests are performed yearly by an independent security firm. If stipulated in the service contract with a confidentiality section, customers may request these documents once per year as required.

Privacy Policies

The Qualtrics online privacy policy covers the use and disclosure of personal information that may be collected anytime a user interacts with Qualtrics. Such interactions include visiting any of our web sites, using the Service, or when calling our sales and support departments. A detailed privacy statement is found at the www.qualtrics.com site. In addition, the Terms of Use state acceptable policies regarding the Qualtrics Services.

HOW WE PROTECT YOUR INFORMATION

Qualtrics takes preventative measures to protect all customer information, both programmatically and through employee training. All employees must attend yearly security awareness programs (covering privacy, security, and other policies) and sign confidentiality agreements. Security updates and reminders are sent to all employees quarterly.

VERIFICATION OF POLICIES AND REGULATIONS

All policy verification is handled through the security and compliance departments. Qualtrics has established internal procedures to review, identify, and track compliance of policies, risk management objectives and regulatory issues. Our Security Officer is a certified member of the International Association Privacy Professionals, and disseminates privacy and regulatory concerns to senior management and the company as a whole.

COMPANY POLICIES ON THE WEB

Privacy, legal, and appropriate usage policies are at the bottom of nearly every Qualtrics web page. These are standard in the SaaS industry. The Terms of Service must be acknowledged by every Qualtrics end user, and uses common language to explain acceptable use of our Service. Any conflicting sections in a customer signed service agreement supersede the Terms of Service.

PERSONAL INFORMATION AND DATA PRIVACY

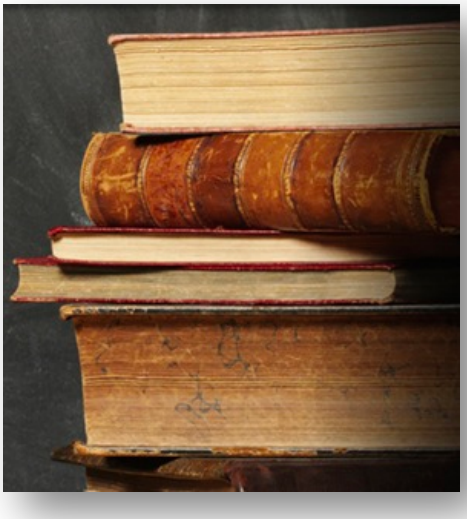
Keeping Personally Identifiable Information (PII) and Protected Health Information (PHI) safe is an important topic with privacy officials these days. Countries around the world are creating their own policies, and not all align with the EU privacy directive. The U.S. is considering a nationwide PII law. But for now, most U.S. states have their own rules and regulations.

Qualtrics protects all data the same, without regarding to type or classification, with the highest level of security systems and processes.

SAFE HARBOR

Qualtrics' privacy and data security policies are compliant with the guidelines of the European Union via the Safe Harbor Agreement. Any data transmitted to our U.S. data centers by a European customer/respondent is processed according to Safe Harbor laws (http://export.gov/safeharbor/).

Certifications / Standards



Qualtrics creates general purpose software products whereby the customer owns and controls their data and users. Therefore, Qualtrics expressly disclaims any knowledge of the data input to its Services, and does not classify data; all data are considered highly confidential, treated equally, and protected using industry best security practices.

An analogy is when a person rents a storage unit. The storage company does not know what is placed in that space *(contents invisible)*. However, the company does have an obligation to provide adequate protection *(security controls)* so that no unauthorized person enters the premises *(data center)*. And the unit owner must secure the unit with a strong lock (*password and access controls)*.

That is why Qualtrics cannot sign any document that requires us to perform in certain ways based upon specific data types defined by a customer or a government.

SSAE-16 SOC 1 TYPE II DATA CENTERS

All Qualtrics hardware (firewalls and servers) and data are located in SSAE-16 Service Organization Control 1 Type II audited data centers. Detailed reports may be requested by existing customers from the data center (listed above) or from Qualtrics with a signed confidentiality agreement.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Qualtrics adheres to the OWASP ASVS methods for development and code review.

FIPS SECURITY REQUIREMENTS

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," states the basis for sound security practices in any organization. Qualtrics meets all requirements as listed in section 3, such as awareness and training, incident response, media protection, and risk assessment.

There is a separate document that details how Qualtrics utilizes those requirements: "Qualtrics & Federal Standards White Paper."

HR Policies

Qualtrics' rapid growth requires an influx of great talent. All new hires are held to rigorous standards of talent and proven track records. Qualtrics also requires background checks and adherence to strict privacy guidelines, except for Barnaby, the company dog.

POLICIES

Upon hire, all Qualtrics employees are required to sign a privacy and confidentiality agreement that specifically addresses the risks of dealing with sensitive digital information. The policy includes the prohibition of access to customer data without customer permission. This permission is typically granted in the context of technical support for survey design. Any employee found to have violated this policy will be immediately terminated and legal action may result.

PROVISIONING ACCESS

Practical access (different than granted access) to customer accounts is only given to those with a legitimate business need. This includes members of our support team, members of our engineering team for specific debugging issues, and select members of our sales teams that handle creating accounts for new customers. All system and service accesses are logged.

QUALTRICS SECURITY TEAM

The Qualtrics Security team comprises personnel from engineering, IT, HR, and legal departments. The Site Reliability Engineers are responsible for securing and monitoring hardware at the data centers. This includes router/firewall configuration, cage security, and reliability verification. Internally, the IT department ensures workstation and local server security. HR is responsible for performing background/criminal employee checks. The Legal team ensures a safe work environment and that security plans are reviewed and followed. They also monitor security and privacy violations.

TRAINING

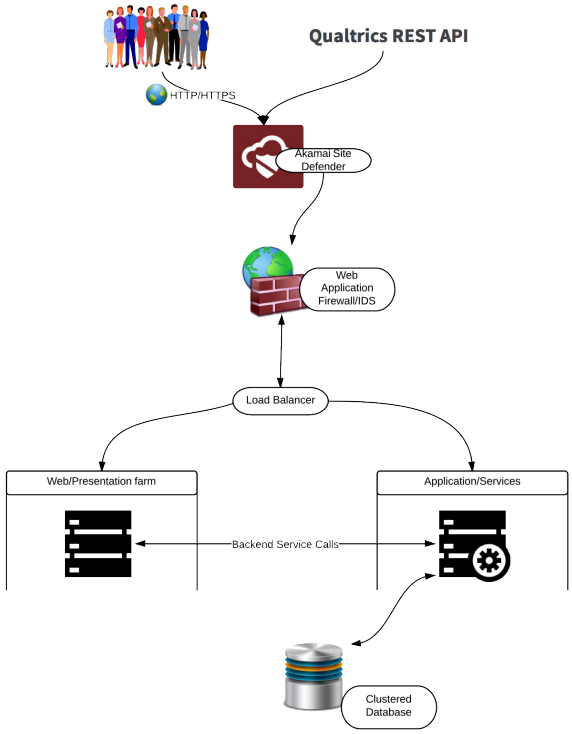
Qualtrics employees are formally trained each year on company policies and security practices, and more frequently in email. This includes Security Awareness training and quarterly updates. All employees are instructed to immediately report possible security incidents to their manager, supervisor, and company director. The computer security section of the employee manual includes privacy and security-related topics.

Network Design, Access, and Location

DATA FLOW AND NETWORK DIAGRAM

In simple terms, transactions involve three parties—the customer, the respondents, and Qualtrics services. The diagram below shows the interaction between these parties.

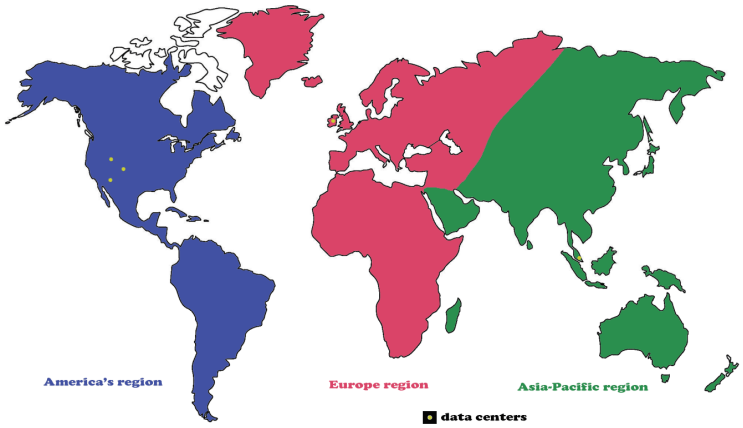
Respondents submit data using HTTPS (TLSv1.2 with AES 128/256 depending on browser) to the front-end web server (usually *customername.*qualtrics.com). Data are processed by application servers and sent to database servers for storage. Web data are delivered to the respondent in the form of survey questions, graphics, and other content created in the survey design. Some surveys are restricted by password or location, as setup by the survey creator. This three-tiered architecture has multiple layers of hardware and software security to ensure that no device/user can be inserted into the communication channel.



LIST OF PHYSICAL LOCATIONS

Qualtrics leases space in three U.S. data centers linked by fiber optic links for redundancy. They are located in seismically low zones, and in areas least susceptible to mother nature's whims. In the U.S., Qualtrics owns and operates all server, firewall, and router hardware/software. Hardware in other locations is managed by the data center staff, but the core operating systems and data are always controlled by Qualtrics. *Data center personnel have no authorization to access Qualtrics data or underlying software environment* (as per mutual agreement and confirmed by SSAE-16 SOC audits).

All customer data are stored within the region where the customer's primary data center resides. In other words, all European customers will have their data stored in a European data center. At no time will Qualtrics knowingly move that data out of the EU. The graphic below shows the Qualtrics geographical regions.



KEEPING THE BAD GUYS OUT

Qualtrics deploys high-end sophisticated firewall systems, physically segmented back-end systems, and high-level security on workstations. Email and attachments are filtered and quarantined before sent to a user. In order to prevent denial of service attacks, we use Akamai perimeter and monitoring solutions. Any detected attack will be thwarted, and services will be switched to new systems so downtime is minimal.

Corporate Policy And Controls

Qualtrics has policies that describe controls/procedures for changes, audits, and incidents. These controls are intended to minimize damage in the event of a disaster or service incident.

CHANGE MANAGEMENT

Qualtrics strikes an interesting balance between controlling change and responding quickly to business needs. Though Qualtrics is a small company, we make nimble business decisions while maintaining our commitment to maintaining the highest standards as our products mature. Thus we have adopted the following base conditions:

- System uptime is most critical
- The system must scale as number of users and amount of data grow
- Features cannot break with a new code release

We conduct studies and perform analyses before any significant change is made. The API, for instance, can be expanded very quickly, but we're hesitant to change the way a particular request works. We maintain legacy requests when superseded by new requests.

INTERNAL NETWORK AND SYSTEMS

Each component of our infrastructure (operating systems, workstations, routers, servers), both internal and in the data centers, have baselines that include security settings and default applications.

All employee data are stored on internal servers, and no customer data are allowed to be stored on the workstation's hard drive (by electronic and company policies). Access to USB media devices and internal DVD drives is disabled. Instant Messaging is restricted to internal company communications using Google Talk.

INSURANCE

Qualtrics' insurance covers general liabilities including loss or compromise of data, errors and omissions, and other liabilities. A list of coverage is available when negotiating sales contracts.

Prevention Of Unauthorized Access

There is nothing more important to Qualtrics than protecting customer data. Qualtrics has implemented innovative methods to prevent unauthorized access to data and the systems that host the data. It starts with having documented security baselines for every component located in the data center, and ends with reinforcing security throughout the organization.

SEGREGATION OF DATA

Qualtrics' services utilize sophisticated databases for the storage of customer data. To best optimize hardware and software, customers are segregated into different virtual areas within the databases. All data are encoded so that only the correct data will be sent to the requesting user. Access to data requires direct ownership (the user who created the survey) or indirectly with rights to the survey (e.g. Brand Admin).

USER ROLES IN THE SERVICES

These roles are found within Research Suite. Other products have similar roles. More details may be found in the University (support) section at the Qualtrics web site.

User— A role that has access to log into the Qualtrics Research Suite for creation and distribution of surveys as well as viewing and analyzing data, as allowed by specific user settings and permissions.

Brand Administrator— For Qualtrics licenses with multiple user accounts, a Brand will be established. This is an administrative level of organization that will contain all users within the license. A Brand Administrator has permissions to log in as any user within the brand as well as restrict the user permissions of any other user in the Brand. Brand Administrators also have access to other administrative tools, such as a password reset function for users within the Brand. This role will be assigned to a person or persons within your organization.

Division Administrator— Has all the same access as Brand Administrators, but only within a Division, an administrative level organization that is a subdivision of the Brand. Such Divisions can be established by a Brand Administrator.

Support Environment— When a Qualtrics user would like help from Qualtrics and interacts with our QUni support team, they may grant a support representative temporary access to the account. QUni will typically view an individual survey in order to give advice or isolate a problem. This option may be disabled by the customer for a period of time or permanently. All Qualtrics employees have unique IDs; no user IDs are shared. And all access is logged.

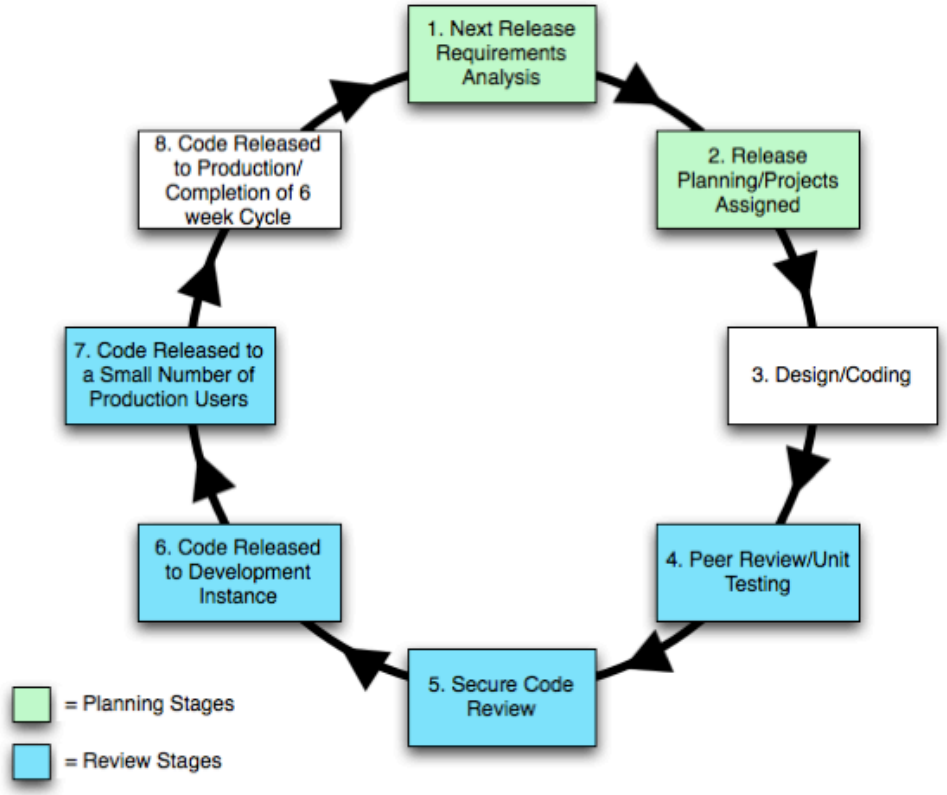
Development Practices

The security of a platform hinges on developing solid and secure code. Weak code makes for a weak product. Here, we'll discuss our development practices.

DEVELOPMENT RELEASE CYCLE

Qualtrics uses an agile development model. This means that we take an iterative approach to software development and remain nimble in responding to the needs of our customers. Code is released on a two-week cycle that includes new features, bug fixes, and upgrades.

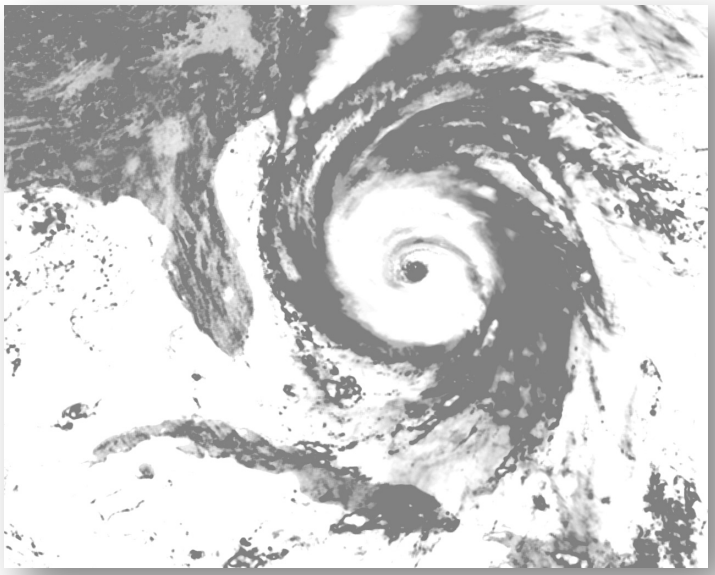
Each cycle includes comprehensive security checks to ensure that the code is vulnerability free. These checks include automated software assessments, peer and managerial reviews. The Software Development Life Cycle (SDLC) is shown below in the diagram.



SEGREGATION OF RESPONSIBILITIES

There are many distinct Qualtrics programming teams, and each team is responsible for specific areas of the production. Engineers may only develop code in their area. This ensures a more secure and reliable development environment. Only specific engineering managers may upload code to production systems.

Disaster Recovery



This section describes the Disaster Recovery Plan (DRP, that includes Data Loss Prevention or DLP) that the company will follow in the event of a disaster that would affect our data or operations. A detailed internal document is used by engineers that contains specific details building, testing, and responding to disasters.

The purpose of the Disaster Recovery Plan is to ensure prompt and complete return to normalcy in the event of a service-affecting disaster. The objectives of this plan are to ensure that 1) in event of disaster, usability is restored promptly with little to no disruption for the end user, and 2) in the event of disaster, data loss is avoided through extensive backup measures.

Disaster recovery and business continuity plans are tested at least annually.

Business Continuity

Qualtrics has a detailed Business Continuity plan in event of a disaster. Though details of the plan are internal, below is a summary of how key business operations will operate following a disaster. This information supplements the information above in the Disaster Recovery section.

PURPOSE

The purpose of this business continuity plan is to ensure prompt and complete return to normalcy in the event of a service-affecting disaster.

GOALS AND OBJECTIVES

The objectives of this plan are to ensure that a) in the event of a disaster, usability is restored promptly with little to no disruption for the end user, b) in the event of disaster, data loss is avoided through extensive backup measures, and c) all necessary support functions of the organization continue.

AKM