Qualtrics Security

White Paper

Why should I trust Qualtrics with my sensitive data?

Revised January 18, 2013
Version 2.0—Prepared for Distribution

Contact security@qualtrics.com for clarification or supporting documentation.

Table of Contents

Introduction

WHAT IS THE PURPOSE OF THIS PAPER?

This whitepaper is intended to answer the majority of your questions regarding the security, reliability, and availability of Qualtrics services. We'll outline the flow of data as you use Qualtrics to collect survey responses, and address the security measures we've taken to protect each part of the process.

WHAT IS QUALTRICS?

Qualtrics is a Software-as-a-Service platform for the creation and distribution \of online surveys and related services. The platform records response data to the cloud, and performs analysis and reporting. All services are on-line and require no download software. Most popular browsers are supported. Qualtrics offers three products for online data collection: the Qualtrics Research Suite, Qualtrics 360, and Qualtrics Site Intercept.

OVERVIEW OF DATA SECURITY

Qualtrics' most important concern is 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 and redundant hardware. Multiple backups are performed nightly.

Qualtrics offers Transport Layer Security (TLS) encryption (also known as HTTPS) and survey security options like password protection and HTTP referrer checking. Our data is hosted by third party data centers that are SSAE-16 SOC II certified.

Security within the Qualtrics Research Suite

Qualtrics services allow clients to control individual permissions of their accounts and surveys. This means administrators can decide who creates, distributes, and analyzes their surveys.

Our service level standards

Qualtrics serves thousands of world-wide businesses, universities and other organizations. As a result, Qualtrics must maintain the highest service levels and create environments to minimize downtime. In the past two years, Qualtrics maintained up-time in excess of 99.97% for all users.

Disaster recovery plan

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. More about the disaster recovery plan is detailed below.

Our commitment to data security

Keeping customer data secure is of paramount importance. Many of our clients demand the highest levels of data security and have tested our system to be sure it meets their standards. In each case, we have surpassed expectations and received high praise from elite companies. All Qualtrics accounts are password protected and all data are replicated in real-time.

WHAT TYPE OF DATA DOES QUALTRICS HANDLE?

There are many types of data that surveys collect, and generally fall into one of the following categories:

1. **RESPONSE DATA** —Data that your respondents provide by answering the questions in surveys.
2. **PANEL DATA**—A panel is a list that Qualtrics can use for the distribution of surveys. This usually includes email addresses paired with a name, but can include additional information. Use of panels is optional.
3. **USER INFO**—The requisite name, email/username, and password for logging into Qualtrics. Qualtrics also logs user activity within the tool.
4. **SURVEY DESIGN AND OBJECTS**—Surveys you create along with any graphics and other property hosted by Qualtrics for use in your surveys. You may store graphics and other objects in a library.

WHO OWNS THE DATA THAT QUALTRICS HANDLES?

Clients maintain ownership of all surveys, response data, panel data, and user information. We maintain the right to collect usage statistics (such as number of responses collected) and audit logs to help provide a great user experience.

Privacy Policy

The Qualtrics policy statement covers the collection, use, and disclosure of personal information that may be collected anytime a user interacts with Qualtrics, such as when visiting our Web site, using the service, or when calling into our sales and support departments. A separate document which only addresses this policy is available by request.

WHY WE COLLECT PERSONAL INFORMATION

Qualtrics collects personal information for purposes of software licensing, billing and practices related with selling or distributing the software. In addition, private information may be necessary to deliver a superior level of customer service. It enables us to provide immediate solutions to problems and focus on individual interests. A user's personal information allows keeping up-to-date on the latest software features, special announcements, and events.

WHAT INFORMATION WE COLLECT AND WHY WE USE IT

We do not sell or make available specific information about our clients or their clients, or their data, except in cooperation with law enforcement bodies in regards to content violations or violations of applicable laws. We maintain a database of user information which is used only for internal purposes such as technical support, notifying members of changes or enhancements to the service.

Qualtrics Users

Qualtrics users transmit data to Qualtrics' servers. Whether this data is collected anonymously, or personal information is disclosed, all Qualtrics users are responsible for the data they collect. We advise users to be sensitive to privacy concerns, and address disclaimer explanations as they deem appropriate. Brand Administrators control the brand, including users, look and feel, and collected data. Qualtrics is not responsible for any data lost or stolen through hacking or negligence by client users.

Customer Training and Support

Qualtrics may ask for personal information or account access when support calls are requested, either by phone or email. We also may ask for personal information when registering for a meeting, participating in an online survey, or purchasing a Qualtrics license. Further, Qualtrics may access a user's account to resolve or investigate a software issue within the system or account. If the client does not wish a Qualtrics support person to access their account, that permission may be disabled by the Brand Administrator.

Client Relations

Qualtrics reserves the right to contact our clients for marketing purposes.

Web Practices

Qualtrics collects and analyzes aggregate information of visitors, including the domain name, visited surveys, referring URLs, and other publicly available information. We use this information to help improve our Web site and services, and to customize the content of our pages for each individual customer. In addition, Qualtrics reads browser languages and settings in order to customize surveys for respondents.

Billing Process

Qualtrics uses secure third party services for online credit card payment processing. Qualtrics does not record or store credit card information on our site or servers.

WHEN WE DISCLOSE YOUR INFORMATION

Qualtrics takes all privacy matters seriously. Qualtrics does not sell or rent contact information to other marketers or vendors. Any disclosure of information within Qualtrics is to help us provide superior service or to remedy customer service issues. Personal information may be shared with certain entities in connection with the outlined privacy policy. Qualtrics reserves the right to transfer personal identification information within the company throughout the licensing process, For example, from sales staff to accounting and support. We may disclose client information as legally required by law enforcement or governmental agencies for national security, law enforcement, or other issues of public importance.

HOW WE PROTECT YOUR PERSONAL INFORMATION

Qualtrics takes preventative measures to protect your personal information. In training procedures and corporate processes, employees are educated on the outlined privacy policy and required to abide by it. All employees must attend security awareness programs and sign confidentiality agreements.

PROTECTING CHILDREN

Qualtrics does not knowingly collect personal information from children under 13 for marketing purposes. Qualtrics is not responsible for any survey data collected by client users, including sensitive data, collected by those under 13. If a child under 13 submits personal information directly to Qualtrics and we learn that that personal information is the information of a child under 13, we will notify the Brand Administrator and ask that the data be removed.

METHOD OF VERIFICATION OF OUR POLICY

All verification is though in-house processes. Qualtrics has established an internal procedure for an annual objective review to ensure continued compliance with privacy and other policies.

HOW WE INVESTIGATE UNRESOLVED COMPLAINTS AND DISPUTE POLICY

In the event that a user feels Qualtrics' privacy policy has been violated, requests for a formal inquiry may be sent to support@qualtrics.com. Qualtrics will assign a case manager and provide all necessary documentation for review. Within 30 days of receipt of a request, the case manager will conduct a formal review, prepare a report of findings and provide it to the user that requested the review. In the event that violations of this agreement are discovered, Qualtrics will immediately seek a solution to the violating actions. The conditions set forth in Qualtrics Acceptable Use Statement IV.6. shall govern any action that follows an inquiry.

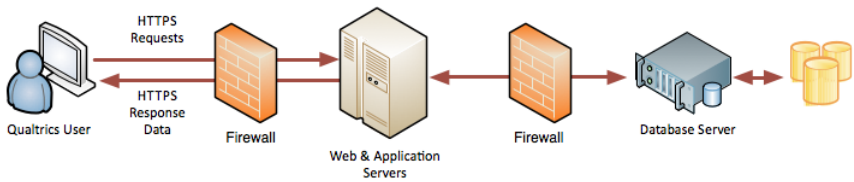
STATUTORY BODY THAT HANDLES PRIVACY QUESTIONS OR DISPUTES

The Federal Trade Commission has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy.

Context and Definitions

DATA FLOW AND NETWORK DIAGRAM

With Qualtrics, the data flows between three important parties—the client, the respondents, and Qualtrics. Throughout this document we'll refer to particular interchanges and storage locations as outlined here.

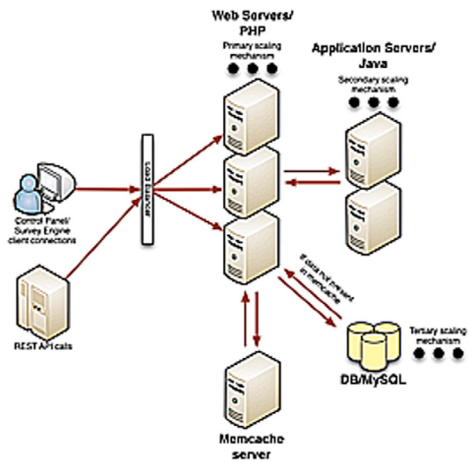


Respondents submit data using HTTP or HTTPS depending on the organization settings. The default is HTTPS (SSLv3 also known as TLSv1). Data are processed by application servers and sent to database servers for storage. Web data are delivered to the respondent in the form of survey questions, graphics, and other content created in the survey design.

Survey creators access the Qualtrics control panel and data in a similar way.

Unless otherwise requested, all client data stays within the region in which the organization resides. In other words, all European clients have their data stored in a European data center.

Below is a general diagram of the back-end systems that process and store data.



LIST OF PHYSICAL LOCATIONS

Qualtrics HQ: Located at 400 W. Dynix Dr. Suite #100, Provo, Utah, United States. All support and development are located here, as well as most salespersons.

C7 Data Center: This is a secure facility that hosts most client data, especially for clients located in the U.S. It is located in the Lindon, Utah.

AWS Data Centers: These are secure facilities that also store client data for specific regions. Locations include Northern Virgina (USA), Singapore, and Ireland. They are owned and operated by Amazon Web Services (aws.amazon.com).

USER TYPES

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.

Multi-Brand Administrator: Has all the same access of a Brand Administrator for All Qualtrics Brands. Also has ability to create Brands and modify settings at Brand level. This is restricted to Qualtrics employees working in a support capacity or in the Engineering team. No access will be made to data without express permission from data owner.

Applicable Certifications / Standards

HEALTH INSURANCE PORTABILITY AND ACCESSIBILITY ACT (HIPAA)

Qualtrics doesn't hold a HIPAA certification because we are not a covered entity. We can, however, be used by covered entities, those who are required to comply with HIPAA privacy rules, for certain applications. We also take appropriate measures to protect PHI such that we may be listed as a health care clearinghouse.

Related to HIPAA is HITECH, Health Information Technology for Economic and Clinical Health Act (HITECH). These new rules require the use of assessments to ensure that data are encrypted and best security practices followed. By using secure data centers, Qualtrics is one secure component for the HITECH requirements.

Clients must monitor their data and enforce their own policies regarding HIPAA requirements. Qualtrics does not recommend storing PII in survey responses.

PAYMENT CARD INDUSTRY DIGITAL SECURITY STANDARDS (PCI DSS)

Qualtrics doesn't hold a PCI certification. We do not process financial transactions and recommend that users do not use Qualtrics to collect credit card information. We do, however comply with the basic DSS requirements and use data centers that are PCI validated service providers.

SSAE-16 SOC II

All Qualtrics hardware (firewalls and servers) and data are located in SSAE-16 SOC II accredited data centers. The reports may be furnished upon request from the data center (listed above).

ISO 27001/27002

These standards, maintained by the International Organization for Standardization, specify requirements and best practices for managing company and customer information. Qualtrics adheres to the principles set forth in these standards, and perform regular audits/verifications on internal systems and procedures.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

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

SARBANES-OXLEY (SOX)

Qualtrics is not a publicly traded company and is not required to undergo SOX evaluations that primarily audit financial controls.

EUROPEAN UNION SAFE HARBOR

Qualtrics' privacy and data security policies are compliant with the guidelines of European Union via the Safe Harbor Agreement. All data created in an organization's region stays within that region.

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 202, "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.

HR Policy

Full-time Qualtrics employees is the norm. We do not employ temporary employees or third-party contractors for any day-to-day work. This allows Qualtrics to maintain the control and quality that our users expect.

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 extensive background checks and adherence to strict privacy guidelines.

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 client data without client permission. This permission is typically granted in the context of technical support. Any employee found to have violated this policy will be immediately terminated and legal action may result

BACKGROUND CHECKS

Qualtrics performs background checks on all applicants as a hiring condition. No Qualtrics employee will ever have any access to client data before these checks are performed.

Certificates

All employees are confirmed to have the degrees and certifications that they purport and/or are required to have.

SSN Verification

All employees are verified legal US workers, and Social Security Numbers are verified.

State and Federal Criminal Background

All employees are checked against State and Federal databases for criminal history.

PROVISIONING ACCESS

Practical access (different than granted access) to client data is only granted to those with a legitimate business need. This includes members of our support team, members of our engineering team, and select members of our sales teams that take care of creating accounts for new Qualtrics clients. This access is called multi-brand administration. All access to multi-brand administrative accounts is not possible from outside the HQ location.

REVOKING ACCESS

As soon as administrative access to Qualtrics is no longer required for job responsibilities, it is revoked. This includes termination of employment as well as changes to role or responsibilities in the company. This process is completed within 24 hours of a role change, or at the time of involuntary employment termination.

TRAINING

Qualtrics employees are trained periodically on company policies and security practices at least annually.

Corporate Policy And Controls

In addition to the controls in place to protect against individual employees misusing data, we also employ policies and controls at a company level. These controls are intended to prevent and protect you from potential negative effects of our business management.

CHANGE MANAGEMENT

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

- The system can never go down
- 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 AUDITS/TECHNOLOGICAL ASSET INVENTORY

All the policies in the world won't accomplish much without a trustworthy team verifying compliance. Qualtrics conducts internal audits of several policies on a regular basis, at least twice per year.

Workstation Checks

Ensure that all employee workstation settings are set to high security, no unauthorized software installed, all data stored on servers (not the local drive).

Clear Desk Checks

Ensure that no passwords or other sensitive information are stored on employee desks in plain sight.

Physical Asset Inventories

Ensure that all Qualtrics owned hardware is accounted for, and no rogue hardware is installed on the internal network.

Digital Asset Inventories

Ensure all software is properly licensed, and detect unauthorized software installed on workstations and servers.

Access Control Audits

Ensure that no unused administrative accounts linger. Ensure that employees have appropriate (minimum) levels of access.

Wireless/External Access

Ensure that wireless networks do not connect to internal systems. All external access to internal systems are by two-factor VPN, and limited to employees who truly need such access.

INSURANCE

Qualtrics' insurance covers general liabilities including loss or compromise of data.

CLIENT RIGHT TO AUDIT

Qualtrics clients and potential clients have the right to perform non-intrusive vulnerability scans to confirm general security settings. More intrusive scans or penetration tests may coordinated with Qualtrics Engineering.

Prevention Of Unauthorized Access

Qualtrics has implemented various ways of preventing unauthorized access to accounts, data, and systems.

SEGREGATION OF DATA

Qualtrics utilizes a sophisticated database for storage of response data at rest. To best utilize hardware and software, clients are not segregated into different databases; all data are encoded so that only related data can be sent to the appropriate client. Access to the data requires direct ownership (the person who creates a survey) or other rights to the survey. All types of access will be described below.

LIST OF THOSE WHO MAY ACCESS DATA:

The Qualtrics user who owns the survey: This is typically the person who creates the survey. Ownership of a survey can also be transferred by a Brand Administrator.

Members of a group that owns a survey: : Qualtrics supports an organizational unit called a group. Groups are used for collaborative processes and a group (that may contain several users within the Brand) may be designated as the owner of a survey. Members of groups are granted privileges to view data associated with it.

Users the owning user chooses to collaborate with: Individual surveys may be collaborated (or shared) with other Qualtrics users or groups. When collaborating, the owning user can specify which permissions the other users or members of a group should have, including access to view associated data. Access to collaboration functions may be restricted on a per-user basis.

Brand Administrator: The Brand Administrator has the most control over the brand. The Brand Administrator may log in to any user account within the Brand.

Direct Database Access: : Select members of our engineering team have access at a database level. This access is used for creating off-site backups and performing data restorations. This is all done without viewing data.

Support Environment: When a Qualtrics user would like help from Qualtrics and interacts with our Support team, they may grant a support representative temporary access to the account. The support team will typically view an individual survey in order to give advice or isolate potential problems. This option may be disabled by the client for a period of time, or permanently.

Those with physical access to Data Centers or Backups: Physical access to Data Centers is restricted to a limited number of employees. Physical access does not mean access to data. The physical media resides in servers in a locked cabinet. Off-site backups are encrypted and electronically stored on secured servers.

PASSWORD PROTECTION MEASURES

Failed Attempts

In order to block unauthorized access through password guessing, our systems disable an account after six invalid login attempts. Once an account has been deactivated, the account stays deactivated for ten minutes (and reset each time a new log in attempt is performed).

Password Complexity

Qualtrics has a default five character minimum for user passwords. Settings for length, complexity, and periodic password expiration are available at the Brand level.

Forgotten Password Policy

If a user forgets their password, or more than six invalid login attempts (causing their account to become deactivated), they may call Qualtrics support for help. There is also a self-service password reset that sends an email with a link to create a new password.

Development Practices

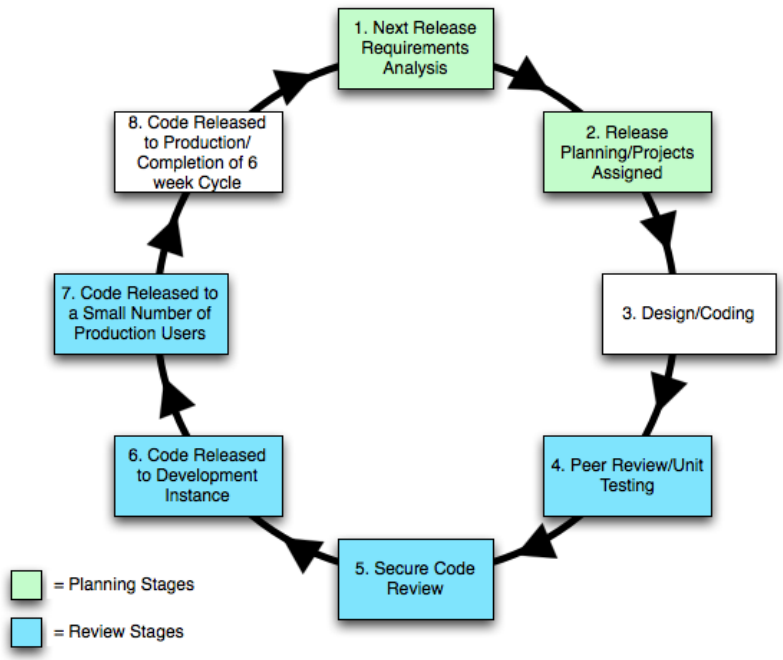
The security of a platform hinges on solid, secure development. Weak code makes for a weak product. Here, we'll discuss our development practices.

DEVELOPMENT RELEASE CYCLE

Qualtrics uses an agile development model. This means that we take an iterative approach to software development and remain very nimble in responding to the needs of our clients. We currently release new code on a six week cycle. This means that every six weeks Qualtrics releases new features, bug fixes, and upgrades.

Each cycle is comprised of an analysis of change requirements, followed by design, coding, unit testing, and acceptance testing. Some projects span several releases before code is published, but the cycle is still followed to ensure frequent benchmarking of progress.

Other projects are more urgent and require implementation as soon as code is developed. These projects typically restore lost functionality or patch vulnerabilities; they may be applied at any time without notification. All other upgrades or changes that affect the interface are preceded by a message delivered via the Qualtrics Message Center (on the My Surveys tab).



DEVELOPMENT (DIGITAL) ENVIRONMENTS

Qualtrics leverages separate instances of the Qualtrics control panel for testing updated code. We use some instances for early candidate code, and one instance for Release Candidate software. This protects your data from ever being controlled or accessed by code still in development.

SECURE CODE REVIEW

Programmers work individually or in pairs developing new code. As the end of each cycle approaches, code is peer-reviewed and tested in a release candidate environment completely separate from our production environment. This testing period allows us to eliminate most bugs before they are ever introduced to production. Code is also inspected for known vulnerabilities. They follow the OWASP ASVS for this secure code review.

SEGREGATION OF RESPONSIBILITIES

The Agile Development Model requires one cross-functional team. This team collectively handles road mapping long-term development efforts, writing code, performing code review, and implementing code to our development and production environments. There are several people within the team who program additions to Qualtrics who also can commit code to our production environment, but code is never implemented without review by other members of the team. Full releases are reviewed by the team at large as described in Secure Code Review above.

CHANGE CONTROL

Our development team is highly cross-functional, so they're in touch with the diverse needs of our clients and the effects of all changes to our code base. New projects and functionalities are planned by a company-wide selection process that takes into account the benefits to our customers. In every change, we carefully analyze impact and retain legacy functionality as long as possible. Leadership within Engineering and our Leadership Team approve all significant changes to Qualtrics products.

Disaster Recovery

This section describes the basic Disaster Recovery Plan that the company will follow in the event of a disaster that would affect our data or operations. A separate document detailing our policies and plans pertaining to disaster recovery in more detail is available upon request.

The purpose of the Disaster Recovery Plan (DRP) 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 a) in event of disaster, usability is restored promptly with little to no disruption for the end user, and b) in the event of disaster, data loss is avoided through extensive backup measures.

POLICIES WHICH PERTAIN TO DRP

1. All client data must be stored at a secure off-site location.
2. Only authorized personnel may access client data.
3. Data security and integrity must be monitored 24x7x365.
4. Backup data must be kept in at least one secondary location.

IT DISASTER DECLARATION CRITERIA

In the event of an emergency, priorities include
1) preserving and recovering as necessary client data on database servers,
2) restoring functionality to firewall and web servers, and
3) restoring support service servers.

LEVELS OF RESPONSE

1) PREVENTATIVE MEASURES—Preventative measures are currently in place at off-site data centers to minimize the effects of a disaster.

2) IT DIRECTOR NOTIFICATION—In event of an emergency at off-site or on-site data centers, the IT head will receive automatic notification via phone and email.

3) COMPANY DIRECTORS NOTIFICATION—If the emergency affects operations, the Qualtrics directors will be notified.

4) RELOCATION OF OPERATIONS—Should the disaster affect on-site operations, all vital systems are stored off-site and are accessed remotely to ensure continuous operations.

REQUIRED AUTHORIZATIONS

Only the IT director has authorization to access physical servers at off-site locations and address problems there. Should the director be unavailable, authorization can be obtained for other available IT leaders to access data.

NOTIFICATION PROCEDURES

Disaster notification comes first to IT director via automatic messaging to email and personal cell-phone. Should the disaster be debilitating, the IT director must contact the Qualtrics directors immediately via phone, and declare a CODE RED emergency. Certain procedures go into motion by all employees to ensure minimal damage and quick restoration.

MEDIA HANDLING PROCEDURES

All media relations will be handled by the Public Relations director. Sensitive information will remain confidential.

KEY DOCUMENTS AND PROCEDURES

There are various internal security policies that are documented and maintained by Qualtrics security department, engineering, and executive staff. These include Asset Policy, Change Management Policy, Security Incident Management, Employee Security Policy, Engineering Security Policy, Software Testing Procedures, and Risk Management Policy.

Business Continuity

A separate document is available upon request that details our plans and policies for business continuity in event of a disaster. Here, we'll summarize how key business operations will be continued following a disaster. This information supplements the information above in the Disaster Recovery section.

OVERVIEW

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.

Benefits

Data integrity and availability along with necessary support functions within the organization will enable us to maintain a trusting relationship with our clients even in times of disaster.

Policies

1. All business continuity activities shall be coordinated through the Qualtrics directors.
2. Backup data must be maintained at off-site locations to mitigate risk of losing critical data.

Overview

Communication coupled with data backup and supply storage form the framework for business continuity. The steps described below will ensure successful continuity in times of disaster.

Backups

Your data is backed up by Qualtrics automatically with two methods: Automatic propagation across servers (immediate upon collection) and daily complete off-site backups.

AUTOMATIC PROPAGATION

Each of the data centers Qualtrics uses for data storage employs technologies that record all data to more than one physical device. This process is accomplished as soon as data is placed there, typically within a few seconds. This protects against periodic failure of the storage devices used.

PERIODIC BACKUPS

Qualtrics additionally makes a full daily backup of all production data. These backups are stored at alternate data centers in the region for which they were created. The backup file is encrypted and compressed.

DATA RETENTION

All Qualtrics data is immediately propagated across several physical storage devices. The data in our production environment is retained until we receive a request to delete it. This deletion immediately flags the corresponding sectors of storage as available for overwriting, and the data is no longer available to Qualtrics or any other party.

The daily backups are retained for one year. Media containing outdated backups are erased according to a US Department of Defense compliant 3-pass overwrite standard. This media is then reused for additional backups or physically destroyed. The backups are manually cataloged and labeled for content.

Should you terminate your service contract with Qualtrics, client data are retained in production environment until requested to be erased. Clients always have the ability to backup their data.

RESTORATION OF DATA

The backups are tested for consistency at least monthly by performing test or actual restorations to production from off-site backup media.

Electronic Security

Below are details of key security controls implemented at Qualtrics.

CONTROL	QUALTRICS' USE
Data Redundancies	• Separate servers at different locations back up data through replication services. • Nightly alternate location backups stored at a secure location. • DBA ensures a hot spare of all active databases, which can be put into use within minutes of the primary's failure. Secondary backups of vital data will be kept off-site and can be restored within 8 hours.
Intrusion Detection	• OSSEC IDS runs continuously on all production servers, including our firewalls. • Nagios is used for immediate alerts to all abnormal activity. • 24x7x365 Detection of malicious activity • 24x7x365 Reporting and monitoring of all activity and all network access points • 24x7x365 Alert signature and system management • 24x7x365 Proactive protection through alert signature and system management • Regular reviews / audits of all user logs
Access Control	• Passwords stored using one-way, salted encryption • No remote software is installed on Workstations. • Secured login, passwords are encrypted, non-disclosure of full ID's on-screen, automated log-out • Session activity is terminated when a security-related parameter has been exceeded or violated.
Application Software	• Our servers run under the Linux operating system and use Apache Web Server, SQL Database, and other solutions written in PHP, and JAVA. All applications are developed and designed first for security. • Audible and text alert systems are in place and triggered if any "critical issues" occur, such as when the site is inaccessible, or when an alternate power supply is activated. Monitoring system extends off-site to IT Administrator.
Testing Environment	• All new applications and extended features go through three levels of testing: 1) Application is tested on development machines by developers 2) Testers verify application functionality in an environment that mimics the end user environment. 3) Application is tested in a production environment with a panel of real-world users.

CONTROL	QUALTRICS' USE
Authorizations	• Authentication is HTTPS SSL compliant. The client's web browsers needs to support 128-bit SSL encryption. SSL 3.0 or better is required. • System can be extended to work with LDAP, CAS, Token, or Shibboleth.
Demographics / Server Load	• Increased load would be handled by increased throttling techniques or eventually requesting more bandwidth from our Internet Service Provider. • Server machines can easily be added to accommodate the application load. • Some clients have dedicated machines for their service (including some or all of the following, dedicated database server, web server and/or other dedicated security measures. • Qualtrics guarantees industry standard annual up time of 99.9%. This is detailed more extensively in the license agreement.
Load, Stress and Penetration Testing	• Apache bench utility and other in-house tools are currently used to conduct load, stress, and penetration testing. • 2012 benchmarks show that Qualtrics runs at 10% of current capacity for surveys and 50% of current email capacity.
Anti-Malware	Anti-malware (anti-virus) software is loaded on the front-end firewall systems. All incoming packets are checked in real-time. Suspected malware is quarantined and prevented from being downloaded to workstations. Definitions are installed automatically when required.

Physical Security

The facilities that host and serve our digital assets are located in the physical world. We understand that you're concerned about the physical security of all these locations and will outline controls here in tabular form.

WHO HAS PHYSICAL ACCESS BY LOCATION

FACILITY	WHO HAS ACCESS
DataCenters	Employees of operating businesses (AWS and C7) with a legitimate business need.
Internal Server Room (at Qualtrics HQ)	Qualtrics engineers with legitimate business need.
Support Environment	Members of Qualtrics University Team and members of other Qualtrics teams with legitimate business need.
Development Environment	Qualtrics engineers and members of Qualtrics University with legitimate business need.

SECURITY MEASURES BY FACILITY

FACILITY	RFID/ PHOTO ID BADGE	VIDEO SURVEIL-LANCE	24/7 SECURITY GUARD	KEY	BIOMET-RICS	LOGGED ACCESS
Qualtrics HQ	yes	yes	no	no	no	yes (RFID)
Server Room	yes	yes	no	yes	no	yes (RFID and manually logged access to key)
AWS Data Centers	yes	yes	yes	yes (Cabi-net)	yes	yes (manual and automatic logs)
C7 Data Center	yes	yes	yes	yes (Cabi-net)	yes	yes (manual and automatic logs)

Incident Response

An incident in this context refers to any discovery of a malfunction of the tool or a deliberate or accidental mishandling of data. Such incidents require a quick response, and employees practice in simulated CODE RED alerts. A detailed incident response policy is maintained by the security department.

A SECURITY INCIDENT INCLUDES:

- The loss or theft of data or information
- The transfer of sensitive or confidential information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without the organization's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system
- The unauthorized use of a system by any person.
- Loss of service
- System malfunctions

RESPONSE TEAM

Our response team is comprised of members of our support and engineering teams who have expertise in technical issues, digital security, and Qualtrics code. One part of the response team, called engineering-on-call, is available for emergency response 24 hours a day 365 days a year.

ISSUE LEVELS

In our effort to appropriately deal with incidents, we've developed a scale for identifying those most urgent to deal with. For your information, please refer to the summarizing table below.

Issue Level	*Typical Conditions*	*Resolution Timeline*
1	The problem may effect individual users in minor ways, may not be reproducible.	Addressed by support team. May or may not be addressed by Engineering.
2	The problem is reproducible and has an impact on usability of the control panel, though a workaround exists to garner full functionality.	Typically addressed within one release (6 weeks +).

Issue Level	*Typical Conditions*	*Resolution Timeline*
3	The problem affects functionality of the control panel or has a slight impact on the survey taking experience.	Typically addressed on or before the next release (less than 6 weeks)
4	A feature of the control panel is effectively unusable, survey taking experience significantly affected.	Will be corrected as soon as code can be developed, typically less than one week.
HC (Hors catégorie)	Key functionality or access to control panel impossible. Survey taking severely hindered or impossible. Potential security threats.	Full Engineering efforts directed toward resolution. After hours, Engineering-on-call will be contacted and will work nonstop until resolution is met, typically less than one hour.

LOSS OR UNAUTHORIZED ACCESS OF DATA

This type of incident will always be categorized as a Level 4 or HC incident depending on scope and severity. Customers will be notified within 24 hours if we discover such a breach.

For this type of incident you'll be assigned a case manager who will work with you in conducting a formal investigation and deliver an official written report within two weeks of the incident. All this is in addition to patches and restoration of data that is placed on priority according to the Issue Levels table.

If you discover a data breach you may also initiate this process by contacting our response team by email at support@qualtrics.com.