Qualtrics Security

White Paper

Why should I trust Qualtrics with my sensitive data?

Version 2.0—August 16, 2011

Qualtrics Security

White Paper

Why should I trust Qualtrics with my sensitive data?

Revised August 16, 2011

Version 2.0

Table of Contents

Introduction

WHAT IS THE PURPOSE OF THIS PAPER?

Your data is important to you. The security of your data is important to us. This paper is intended to answer as many questions as possible about the security, reliability and availability of your data as it's stored in the Qualtrics tool. We'll outline the flow of data as you use Qualtrics to collect survey responses. We'll also address the security measures we've taken to protect each part of the process.

WHAT IS QUALTRICS?

Qualtrics is a web platform for the creation and distribution of online surveys. The platform also records response data to "the cloud" and allows analysis within the online tool or export to common formats like CSV and SPSS. Qualtrics now offers 3 products for online data collection: the Qualtrics Research Suite, Qualtrics 360, and Qualtrics Site Intercept.

OVERVIEW OF DATA SECURITY

Our servers have been tried and tested by most major corporations and government organizations, including the CIA, that demand high level data security.

Qualtrics offers Transport Layer Security (TLS) encryption (HTTPS) and survey security options like password protection and HTTP referrer checking. Our data is stored in data centers that are audited and SAS 70 certified.

Security within the Qualtrics Research Suite

Qualtrics Research Suite allows all clients to control individual permissions of their accounts and their surveys. This means administrators can decide who creates, edits and distributes surveys, and analyzes data.

Our service level standards

Qualtrics serves businesses, universities and other organizations around the world. If one time zone is sleeping, we have users in another that are not. As a result, Qualtrics takes service level standards very seriously and seeks to minimize and eliminate downtime. During the last year, Qualtrics has maintained up-time in excess of 99.97% for all users. Qualtrics is committed to this standard of excellence for all our users, guaranteeing 99.9% up-time.

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. Qualtrics' entire disaster recovery plan is explained in separate document entitled, "Disaster Recovery Plan."

Our commitment to data security

Data security is very important to us at Qualtrics. 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.

Qualtrics has SAS 70 Certification and meets the rigorous privacy standards imposed on health care records by the Health Insurance Portability and Accountability Act (HIPAA). All Qualtrics accounts are hidden behind passwords and all data is protected with real-time data replication.

WHAT TYPE OF DATA DOES QUALTRICS HANDLE?

Qualtrics is a powerful, full-featured data collection tool. There are many types of data you can gather with it, but generally the data falls into one of the following categories:

1. RESPONSE DATA —Data that your respondents provide by answering the questions in your surveys.

2. PANEL DATA—Data that you choose add to Qualtrics as part of a panel. A panel is a list Qualtrics can use for distribution of surveys. This usually includes email addresses paired with a name, but can include as much additional information as you like. Use of panels is completely optional.

3. USER INFO—The requisite name, email/username, and password for logging into Qualtrics. Qualtrics also logs user activity within the control panel.

4. INTELLECTUAL PROPERTY—Surveys you create along with any graphics and other property hosted by Qualtrics for use in your surveys. You can alternatively host graphics and other properties yourself and reference them using HTML statements within the survey design.

WHO OWNS THE DATA THAT QUALTRICS HANDLES?

Your surveys, your data. You maintain ownership of all intellectual property, 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. However, these statistics are calculated in aggregate and never cross into the specifics of your surveys and data.

PRIVACY POLICY

The Qualtrics policy statement covers the collection, use, and disclosure of personal information that may be collected by Qualtrics anytime you interact with Qualtrics, such as when you visit our Web site, when you purchase Qualtrics software and services, or when you call our sales or support associates. Your privacy and data are a clear priority at Qualtrics. 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, such as your phone number, may be necessary to deliver a superior level of customer service. It enables us to give you immediate solutions to problems and focus on your individual interests. Your personal information helps us keep you posted on the latest software features, special announcements, and events that may be of interest to you.

WHAT INFORMATION WE COLLECT AND WHY WE USE IT

We provide the most advanced survey building tools for corporations, research companies, consultants and universities. 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 possessing a court order 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 may transmit private data to Qualtrics' servers through the data they collect. Whether this data is collected anonymously, or personal information is disclosed, all Qualtrics users are responsible for the private data they collect. We advise users to be sensitive to such practices, and address disclaimer explanations as they deem appropriate. Qualtrics users are responsible for their passwords and the information that they collect. Qualtrics is not responsible for any data that is lost or stolen through hacking or negligence by users. To help users with these responsibilities, we provide extensive permission and security controls.

Customer Training and Support

Qualtrics may ask for your personal information or account access when you're discussing a service issue with a Qualtrics associate on the phone or through email correspondence. We also may ask for your 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.

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 your contact information to other marketers or vendors. Any disclosure of information within Qualtrics is to help us provide superior service or fix subsequent 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, e.g. from sales personnel, to accounting, to training, or to 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 when a court order is issued.

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.

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 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 attempt to delete the information as soon as possible.

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 the European Union Safe Harbor Agreement.

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. No later than 30 days after 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

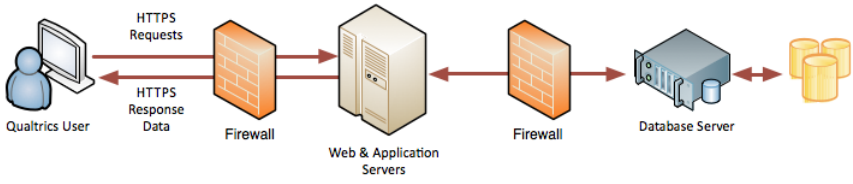
The Federal Trade Commission has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy.

Context and Definitions

DATA FLOW AND NETWORK DIAGRAM

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

As a respondent responds to a survey, the information they provide is submitted via HTTP or HTTPS depending on user settings. The data is processed by our application servers and submitted to our database servers for storage. Web data is delivered to the respondent in the form of survey questions, graphics, and other content you've included in your survey design.



As you access the Qualtrics control panel, you send requests for information via HTTPS and our application servers process the request. The request is passed along to the database servers and the appropriate data is passed up to you through the web and application servers.

LIST OF PHYSICAL LOCATIONS

Business Operations: This facility is located at 400 W. Dynix Dr. Suite #1. Provo, UT, 84604 in the United States. This is where our day-to-day operations are housed. No client serving data centers are kept at this location.

Support Environment: This is an area of Qualtrics HQ where our Qualtrics University team works. This is our external support and training division. They offer free support for all Qualtrics clients.

Development Environment: This is an area of Qualtrics HQ where our engineering team works on improving and maintaining Qualtrics software and systems.

Web Servers: This is a set of servers operated external to Qualtrics HQ, dedicated to hosting website content to the world.

Application Servers: This is a set of servers operated external to Qualtrics HQ, dedicated to running Qualtrics' proprietary code such as the Qualtrics Research suite.

Data Centers: These are secure facilities that store client data. They are located in such diverse locations as Northern California, USA, Northern Virgina, USA, Utah, USA, Singapore, and Ireland.

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: In 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.

Applicable Certifications / Standards

HEALTH INSURANCE PORTABILITY AND ACCESSIBILITY ACT (HIPAA)

Qualtrics does not hold a HIPAA certification because we are not considered a covered entity by the U.S. Department of Health and Human Services as we do not personally use this type of data. We can, however be used by covered entities, those who are required to comply with HIPAA privacy rules, for certain applications. We do take appropriate measures to protect PHI such that we may be listed as the business partner of a covered entity.

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.

SAS 70 TYPE II

Qualtrics only stores data in data centers that have historically received unbiased favorable SAS 70 Type II audits annually. Note that the SAS 70 has been replaced by the Statement on Standards for Attestation Engagements (SSAE) No. 16 and we will adhere to that standard.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT

The HITECH act expands the responsibilities of HIPAA to business partners when it comes to breach notification. Qualtrics will fully comply with all HITECH act requirements.

ISO 27001

This standard is a widely-adopted global security standard developed by the International Organization for Standardization that sets out requirements and best practices for a systematic approach to managing company and customer information. We adhere to the principles set forth in the standard and only use data centers that have demonstrated their adherence by periodic assessments and annual certification.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Qualtrics adheres to the OWASP ASVS methods for development and code review. This means that we take software development seriously and weigh security risks whenever we modify our products.

SARBANES-OXLEY (SOX)

Qualtrics is not a publicly traded company and is not required to undergo SOX evaluations which primarily audit financial controls. However, we do actively review our business operations to ensure we are acting with the highest integrity.

EUROPEAN UNION SAFE HARBOR

Qualtrics' privacy and data security policies are compliant with the stringent guidelines of European Union via the Safe Harbor Agreement. Qualtrics servers maintain protections consistent with the Safe Harbor Agreement.

HR Policy

All daily operation is carried out by in-house Qualtrics employees. 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 concerns and risks of dealing with sensitive digital information. The policy specifically is that access to client data without specific permission is prohibited. This permission is typically granted in the context of technical support and employees outside of engineering and support have no access to customer data. Any use aside from that reasonably required to perform the duties of the job is also prohibited. Any employee found to have violated this policy will be immediately terminated and any applicable legal charges will be raised against them. Retraining in these policies is performed as needed, at least annually.

BACKGROUND CHECKS

Qualtrics performs background checks on all applicants as a hiring condition. No Qualtrics employee will ever have any access to 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.

Former Employment Verification & Integrity Reference Checks

All prospective employees have their stated employment histories verified and their integrity references called.

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 designated machines in our Qualtrics office.

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. In addition, we regularly review which employees have these permissions and make changes as needed.

TRAINING

Qualtrics employees are retrained periodically on company policies as well as best practices for digital security. These trainings are conducted at the team at least annually and additionally as needed.

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. We're committed to maintaining the highest standards as our product evolves. In the case of engineering, we've adopted the following base conditions:

- The system can never go down
- The system must scale as number of users and amount of data we store grows quickly
- All the thousands of existing features cannot break when we release new code
- A large percentage of our engineering effort must be dedicated to keeping existing code current

> *"If we add a 1,000 new features but fail to meet any of these base conditions, we're out of business."*
>
> **—Guiding Philosophy of Qualtrics Development**

Bearing that in mind, significant changes to the product or the way we manage the company are made quickly, but never hastily. We conduct studies and perform analyses before any significant change is made. The API, for instance, can be expanded very quickly, but we're very hesitant to change the way a particular request works. We maintain legacy request formats when they are outmoded by different requests.

INTERNAL AUDITS/TECHNOLOGICAL ASSET INVENTORY

All the policies in the world won't accomplish much without somebody checking for adherence. 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 at defaults, no unauthorized software installed, employee using basic safety precautions.

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, also ensure that no rogue hardware is installed on the internal network.

Digital Asset Inventories

Ensure compliance with licensing of software, also detect unauthorized software installed on workstations and servers.

Access Control Audits

Ensure that no unused administrative accounts linger. Ensure that employees have appropriate levels of 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

At Qualtrics we take the information security of our clients very seriously. We are aware that some individuals or organizations may attempt to gain unauthorized access to information gathered by our clients. Bots (semi-automated programs that carry out repetitive tasks of various kinds according to their design) are often utilized in this process.

SEGREGATION OF DATA

Qualtrics utilizes a sophisticated database for storage of response data at rest. Qualtrics clients are not segregated into different databases or hardware, but all data is appropriately labeled and given permissions for appropriate retrieval. Namely, responses are labeled with a Survey ID that correlates them with the appropriate survey. 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 unfettered access to all data within 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.

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 on a locked cabinet. Off-site backups are stored in a fire safe in a secure room. Access to this room is restricted and logged.

PASSWORD PROTECTION MEASURES

Failed Attempts

In order to block unauthorized access attempts through password guessing, our systems are designed to allow only six log in attempts before an account becomes disabled and further attempts to log in are blocked. Once an account has been deactivated due to failed log in attempts, the account stays deactivated for ten minutes (and reset each time a new log in attempt is performed).

Because bots rely on the ability to endlessly guess different combinations of passwords, the above measures effectively block these programs from gaining unauthorized access to our clients' accounts.

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 enabling clients to enhance password complexity.

Forgotten Password Policy

If a person forgets their password, attempts to log in to their account more than six times (causing their account to become deactivated), they may call Qualtrics support for help. If they do so, they will be advised by the support team to do the following:

1. They will be directed to the login page of their organization where they can click on the "Forgot your password?" link. Clicking on this link and filling out the requested information will cause our systems to send an email to the user provided email address for their account. This email contains a link that can be used to establish a new password.

2. If their attempt to use the link is unsuccessful, they will be directed to their Brand Administrator who will be able to change the password for the user through the administration interface.

3. Should their Brand Administrator be unavailable, a Qualtrics support member will send a message to the email we have on file for the account holder inquiring whether they wish us to enable their account and reset their password. Using this form of email validation, we will enable the account and send a temporary replacement password. The user will then be able to change their password to one of their choice.

Development Practices

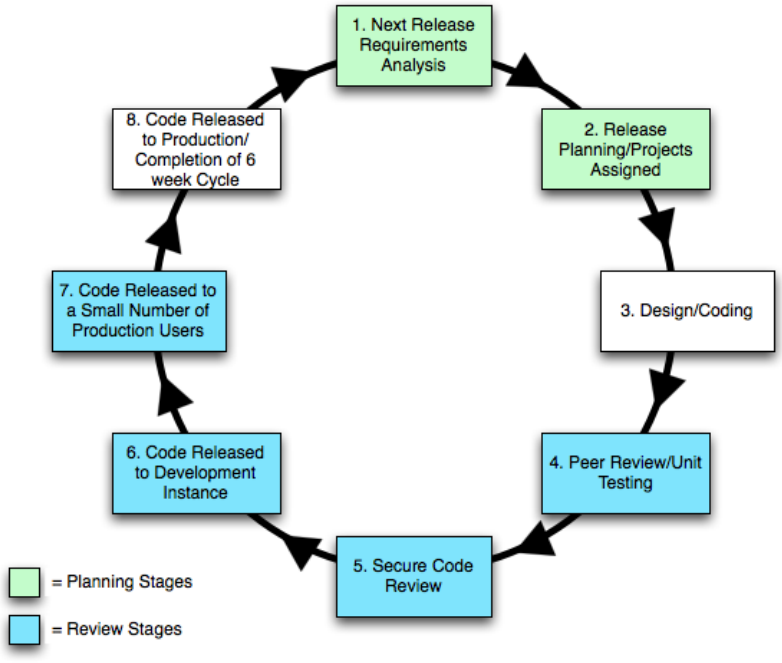
The security of a platform that handles important data hinges on its development. Weak code makes for a weak product. Here, we'll discuss our development practices in some detail.

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 6 week cycle. This means that every 6 weeks Qualtrics releases new features and upgrades. It also gives us frequent windows for releasing fixes to features that do not work as desired. Outside of this cycle we can make "emergency" releases whenever needed.

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 and can be applied to Qualtrics Products mid-release 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. All of our development code runs against "dummy databases" that contain no real customer data.

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

Qualtrics' success depends on the availability and security of its data. In recognition of this, it is vital that we be prepared to respond in the event of a disaster. This section describes the Disaster Recovery Plan that the Engineering Team will follow in the event of a disaster that would affect our data or operations. It includes a summary of how key IT functions will be restored following a disaster. 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 this data.
3. Data security and integrity must be monitored 24x7x365.
4. Backup data must be kept in at least one secondary location to minimize the consequences of disaster.

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 the entire engineering team 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 as necessary, other key employees.

MEDIA HANDLING PROCEDURES

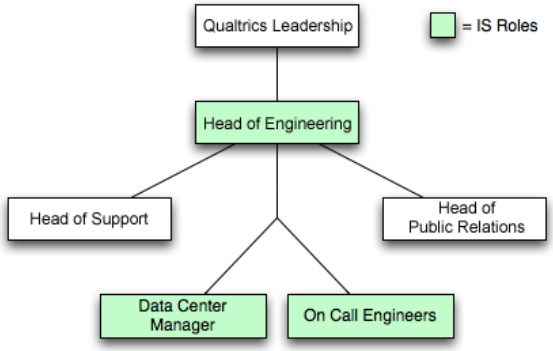
All media relations will be handled by the Public Relations director. Sensitive information will remain confidential.

IT CALL OUT PROCEDURE

IT employees shall be contacted and brought in to the situation according to personal availability and the needs of Qualtrics as determined by the IT Director.

CONTINGENCY MODE RESOURCE PLAN

Functional Disaster Management Organizational Chart



Teams Roles and Responsibilities

1) Off-site Data Center Managers are responsible for maintaining functionality and usability of off-site data warehouses. They are responsible for sustained security, power, and connectivity of our off-site data.

2) IT Director is primarily responsible for initiating and implementing the disaster contingency plan should there be an issue at either of the off-site data locations..

3) Engineering Director shall be responsible for determining the scope of the disaster and for giving clearance to the IT Director to make business affecting decisions.

4) Support director shall be responsible as needed to maintain client relations and ensure continued program functionality following disaster.

5) Public relations director shall be responsible as needed to handle necessary press and client interactions regarding the disaster.

RECOVERY TEAM DIRECTORS	*COMMAND CENTER COORDINATORS*	*RECOVERTY TEAM LEADERS*
IT Director, Qualtrics	Company Directors, Qualtrics	Support Director, Qualtrics
Engineering Director, Qualtrics		Customer Relations Director, Qualtrics

Recovery Teams and Emergency Contact List

The above persons shall be responsible for assembling teams as the situation permits. All questions regarding recovery teams shall be directed to them.

Manpower Recovery Strategy

In event of an emergency affecting Qualtrics employees, part-time and temporary employees shall be called upon to work as available to maintain necessary manpower.

KEY DOCUMENTS AND PROCEDURES

Functional Disaster Management Organizational Chart

OWASP Security Standards Guide (available on internal server).
All other vital documents can be obtained through the Qualtrics internal server.

Off Site Storage Locations

Northern California, USA
Northern Virginia, USA
Utah, USA
Singapore
Ireland

NOTIFICATION AND REPORTING

Notifying and Mobilizing the Teams

Primary notification is automated through the Nagios open source monitoring system. Should further action be needed, the Head of IT is responsible for notifying Qualtrics leadership via phone and email. All further correspondence and mobilization will occur through phone and email.

Notifying Management and Key Employees

As directed above, the Head of IT shall contact Qualtrics leadership, who in turn are responsible for determining the scope of the disaster and determining what further contacts must be made.

Handling Personnel Family Notification

As needed, personnel family notification shall be completed through the employees' respective department heads via phone.

Handling Media

All media requests shall be transferred to the Head of Public Relations.

Maintaining Event Log

Database, web server and OS logs are maintained automatically and are accessible as needed to Head of IT. Application level logs are maintained for critical processes, and are also accessible to the Head of IT.

Phase Reporting

Phase Reporting shall be handled by the Head of IT.

RETURN TO NORMAL OPERATING MODE

Criteria for Returning to Normal Operating Mode

Normal operating mode shall be reinstated when:

1) Proper functioning of all vital servers can be demonstrated in one location. As each location has primary and backup servers, only one location will need to be functioning before returning to normalcy.
2) Utility servers have been tested and function properly.
3) Necessary staffing can be obtained as determined by the Qualtrics directors, IT Director, and Support Director.

Procedures for Returning to Normal Operating Mode

1) Proper functioning of vital servers must be demonstrated in one location. This includes using the fail-over servers and synchronizing with the main servers once data integrity can be determined.
2) Support service servers shall be rebuilt under IT Director's direction.
3) As needed, the previous nightly backup shall be restored.

Procedures for Recovering Lost or Damaged Information

The most recent data or backup shall be loaded onto an off-line computer. Once data integrity has been checked, it shall be integrated back into the system. Notification to affected users by best available means shall be completed within 24 hours.

Detailed Lists, Inventories and Services Required

Detailed inventories of all office equipment and supplies are maintained through the accounting department. These can be accessed as needed.

TESTING OF RECOVERY PLAN

Testing primarily consists of necessary frequent data recovery. Because Qualtrics is deployed on multiple servers, (a) loss of a single server does not cause an outage, and (b) deployment on additional servers is done regularly, in effect testing the recovery plan with each new server deployment.

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

Customer support is our top concern at Qualtrics. 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.

Manpower Recovery Strategy

In the event of an emergency affecting Qualtrics employees, part-time and temporary employees shall be called upon to work full time as available to maintain necessary manpower.

BUSINESS RECOVERY ACTIVITIES AND PROCEDURES

Power and Other Utilities

Because Qualtrics is primarily a web-based company, a temporary loss of power or utilities at our office will not affect business operations. Our data centers feature redundant power supplies to mitigate the risk of power loss. In the event of power loss, on-site batteries will provide up to 30 minutes of power at full server load. An additional diesel generator at locations provide 72 hours or more of full power with onsite fuel, and also contracts are established for priority access to off-site fuel sources.

Premises, Fixtures, and Furnishings

Negotiations will be made with local vendors to purchase necessary fixtures and furnishings should a disaster occur.

Communication Systems

Temporary communications will be conducted via cellphone until the communications provider is able to restore connectivity.

Other Equipment

Computers and other necessary equipment will be acquired through local vendors.

Human Resources

In event of an emergency affecting Qualtrics employees, part-time and temporary employees shall be called upon to work full time as available to maintain necessary manpower. Additional hiring will be conducted to meet sustainability requirements.

Information and Documentation

Information and Documentation is stored both on-site and off-site. Thus no measures will be needed to return to normalcy.

Operations and Administration Support Services

Payroll and other administration support services are conducted via online applications. Thus no measures will be needed to return to normalcy.

RETURN TO NORMAL OPERATING MODE

Criteria for Returning to Normal Operating Mode

Normal operating mode shall be reinstated when:

a) Proper functioning of all vital servers can be demonstrated in one location. As each location has primary and backup servers, only one location will need to be functioning before returning to normalcy.

b) Utility servers have been tested and function properly.

c) Necessary staffing can be obtained as determined by the Qualtrics directors, IT Director, and Support Director.

Procedures for Returning to Normal Operating Mode

1) Proper functioning of vital servers must be demonstrated in one location. This includes using the fail-over servers and synchronizing with the main servers once data integrity can be determined.

2) Support service servers shall be rebuilt under IT Director's direction.

3) As needed, the most recent data image or backup shall be restored.

Backups

Your data is backed up by Qualtrics automatically with two methods: Automatic propagation across servers (immediate upon collection) and periodic scheduled 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. It too enables cross-site failover.

PERIODIC BACKUPS

Qualtrics additionally makes a full daily backup of all production data. These backups are stored on hard drives in a locked server room. The backup file is a compressed database that stores complete survey responses compressed into individual cells. This means that your data is digitally obfuscated by two levels of compression, then stored in the same physically secure facility that houses our source code. The backups are not readable by a human or a machine without knowledge of the compression schemes and our proprietary technology for decoding the response data and matching it to actual survey questions.

DATA RETENTION

All Qualtrics data is immediately propagated across several physical storage devices at rest, and is backed up to an off-site location daily. 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, your data is retained in production environment until you request erasure. You'll have ample opportunity to export data. Backups are still maintained for one year after that point.

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

Qualtrics is an online service provider. Our key controls for your data's security and integrity are digital. Here we'll represent several controls in a tabular format.

CONTROL	*QUALTRICS' USE*
Data Redundancies	• Separate servers at different locations back up data through replication services. • Nightly hard copy backups created and transferred periodically to 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. • Key functions and communications are IP restricted to certain machines and locations.
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.

CONTROL	QUALTRICS' USE
Testing Environment	• All new applications and extended features go through three levels of testing: 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.
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. • 2011 benchmarks show that Qualtrics runs at 10% of current capacity for surveys and 50% of current email capacity.
Anti-Malware	All applicable systems are equipped with anti-malware that updates definitions automatically on a daily basis.

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 with a legitimate business need.
Internal Server Room	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	yes	no	yes (RFID)
Server Room	yes	yes	no	yes	no	yes (RFID and manually logged access to key)
Data Centers	yes	yes	yes	yes (Cabi-net)	yes	yes (manual and automatic logs)

Incident Response

Occasionally, despite rigorous efforts to develop secure code and bug-free products, things go wrong. An incident in this context refers to any discovery of a malfunction of the tool or a deliberate or accidental mishandling of data. We take such incidents seriously and devote a huge effort to limiting their frequency and severity, as well as quickly responding to them.

RESPONSE TEAM

Our response team is comprised of members of our support and engineering teams who have expertise in technical issues, digital security, and the code and functionality of the Qualtrics Research Suite. 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.	ddressed 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 +).
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. You'll 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.