Before reading this material you must agree to the terms. If you do not agree, then you must destroy or permanently delete this document. This document may not be uploaded to any web site that is accessible to the general public or indexed by public search engines.

Terms & Conditions

This document contains information regarding Qualtrics security posture. It supersedes all previous versions. The Qualtrics security team has created this document to the best of its ability, and does not warrant that it is error-free.

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

Although this document is copyrighted, you may distribute this document for the purposes of evaluating Qualtrics’ security posture. The full version of this document requires a confidentiality agreement.
# Table of Contents

Executive Summary ......................................................................................................................... 4
Introduction ........................................................................................................................................ 6
General Privacy Policies .................................................................................................................. 8
Certifications / Standards ................................................................................................................ 10
Human Resource Policies ............................................................................................................... 12
Network Design, Locations, and Assessments .............................................................................. 14
Preventing Unauthorized Access .................................................................................................... 17
Development Practices ................................................................................................................ 18
Disaster Recovery ........................................................................................................................... 20
Business Continuity ....................................................................................................................... 21
Backups – Data Retention .............................................................................................................. 22
Incident Response ......................................................................................................................... 23
Risk Management ......................................................................................................................... 24
Privacy Appendix ........................................................................................................................... 25
Executive Summary

If you read nothing else…

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

All Data are owned and controlled by Customers. Qualtrics is only a data processor, not a data controller. All products are self-service (“do-it-yourself”) whereby the Customer’s Users solely determine: 1) what data to collect; 2) from who; 3) from where; 4) for what purpose; and 5) when to delete it. Qualtrics doesn’t transfer Data; all Data are stored and processed in a single data center, and only for the purpose of providing the Services.

Qualtrics will only process Data to the extent necessary to provide the Services, and does not disclose any Data to third parties.

Qualtrics treats all Data as highly confidential, and does not classify or represent the Data. In other words, we don’t know what information are being collected, and Customers are free to use the software as they wish. We use industry best practices to keep all Data safe from criminals and hackers, and have devised proprietary methods to prevent disclosing Data to the wrong requester due to programming errors.

This document is not static; it will be periodically updated as our processes, procedures, or the security/privacy landscape change.
DEFINITIONS

Throughout this document, “Data” means information entered by a survey respondent, User (survey creator), or the information generated by Customers within the Qualtrics platform. A “Brand Administrator” is the account manager of the Customer account. An account is also called a “Brand.” A “User” is a Brand end-user with a Qualtrics login to create, report on, and send surveys, or otherwise utilize the software (a Brand Administrator is also a User). A “Respondent” is an individual who responds to surveys created by a User. “Responses” are Data collected from surveys taken in web browsers on computer or mobile platforms, or via SMS. A “Customer” means an organization that has a business relationship with Qualtrics. “Services” refers to the range of services provided by Qualtrics, including the software, email, support, and online resources.
Introduction

WHAT IS QUALTRICS?

Qualtrics is an Application Service Provider (ASP) who provides a platform for creating and distributing online surveys, performing employee evaluations, web site intercepts, and other research services. Software-as-a-Service (SaaS) includes ASP software. The platform records response data, performs analysis, and produces reports on the data. All services are online and require no downloadable software, such as browser plug-ins, JVM, or other components. Only modern JavaScript-enabled internet browsers and an internet connection are required. Qualtrics offers multiple products for online data collection: Research Suite, Vocalize, Employee Engagement/360, and Site Intercept. Services include providing the products and technical support. Surveys are usually taken online within a web browser, with optional SMS surveys and offline methods available for smartphones/tablets.

OVERVIEW OF OUR DATA SECURITY

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

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

Qualtrics security practices and operating environments are continuously monitored and assessed. Our processes and procedures to safeguard Data meet or exceed industry standards. The Qualtrics Security and Privacy Officer is accredited by ISC² and IAPP (CIPP/US).

Security within the Qualtrics Services

All Qualtrics products are self-service, and enable Customers to control individual permissions of their accounts and surveys. The Customer designates at least one Brand Administrator who manages the Brand, and that person(s) decides who will create, distribute, and analyze the brand’s surveys. There is also an option to require surveys to first be approved prior to distribution. Account password strength is also controlled by Brand Administrators.

Our service level standards

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

Disaster recovery plan

Within North America, 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. In other parts of the world, each data center has a redundant setup nearby, and is maintained by data center staff. More about disaster recovery and data center locations below.
Our commitment to data security

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

WHO OWNS THE DATA IN QUALTRICS SERVICES?

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

Qualtrics only processes Data to provide the Services. No Data are ever shared or distributed with a third party except as allowed by the Customer. (Exceptions noted below in Disclosing Customer Information section.) And since Qualtrics products are self-service, Data are essentially invisible to our staff; customers operate on their own accord.

DATA CLASSIFICATION/REPRESENTATION

Qualtrics processes all Data the same using industry best security measures designed to prevent unauthorized access and disclosure. Qualtrics does not represent or attest to Data entered into its Services since all Data and User accounts are controlled by the Customer. Qualtrics does not know what Data are being collected, and therefore cannot classify or treat any Data differently. This is beneficial to our Customers, who solely determine how Data should be interpreted and analyzed.

ASSESSMENTS

Automated vulnerability scans are performed regularly with a commercial security provider. Complete penetration tests are performed yearly by an independent security firm.

CUSTOMER TESTING

With prior consent and signed agreement, Customers have the right to perform non-intrusive vulnerability scans or penetration tests on the Qualtrics software. These tests require coordination between the Customer’s account executive, the Customer’s IT/security team, and the Qualtrics InfoSec team. All testing must be performed on the staging environment, not the production environment.

SURVEY SECURITY

There are many ways to protect surveys from being “stuffed,” or being taken by the wrong respondent. Full details are available on the Qualtrics support web site. Surveys may be sent to specific individuals, require a password, or be taken only by Customer employees. It’s up to the Users to determine who should take the survey and what content should be collected. Survey links may be posted on a web page, sent in email, or printed on paper and delivered via certified mail.

Setting a Survey Password

You can set a single, general password that a respondent must enter to access your survey. This is helpful when you are using the Anonymous Link and want to restrict who can enter the survey.

Password Protection: This password protects the survey. Enter password: [password]

If you want to have a unique password for each survey session, you might consider using an Authenticator on your survey.

Preventing Respondents From Taking Your Survey More Than Once

In circumstances where you are offering an incentive or conducting a sensitive survey, you may want to prevent participants from taking the survey more than once.

Prevent respondents from taking the survey more than once.
General Privacy Policies

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

DISCLOSING CUSTOMER INFORMATION

Qualtrics does not sell or rent Customer or other contact information to other marketers or vendors. Any disclosure of information within Qualtrics (as a company) is strictly to assist with technical or service issues. We have high security measures to keep Data safe. We maintain strict control over access to Data. The only employees who are permitted to access Data are those with a business need to know. Qualtrics reserves the right to transfer Customer information within the company throughout the licensing process: for example, from sales staff to accounting.

Qualtrics will only disclose customer information as legally required—either upon a valid court order under applicable law, or to law enforcement or governmental agencies for issues of public importance (for example, national security and time is of the essence). In any case, Customers will be notified as soon as reasonably possible, where allowable by law, if any request is made to disclose their name or any detail of their association with Qualtrics.

HOW WE PROTECT YOUR INFORMATION

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

RESPONDING TO DATA BREACHES

Privacy-related inquiries are handled by various Qualtrics teams or by calling Qualtrics Support. Qualtrics will assign a case manager and provide all necessary documentation for review. Within a reasonable time, or as stipulated by contractual agreement, the case manager will conduct a formal review, and provide the findings to the User that requested the review. Urgent events are processed as soon as possible, and steps taken to mitigate non-compliance or respond to official inquiries. Conditions set forth in the Qualtrics privacy statement, or any specific agreement between Customer and Qualtrics, will govern specific actions. More details in relevant sections below.

STATUTORY BODY FOR 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.

SUBCONTRACTORS

Qualtrics does not use subcontractors to provide its Services.

POLICIES ON THE WEB — ACCEPTABLE USE, PRIVACY, SECURITY

Links to Qualtrics’ privacy and security statements, and acceptable use policy are at the bottom of nearly every Qualtrics web page. Most language is based on industry standards, and tweaked to our ASP business model. The Terms of Service must be acknowledged by every User, and uses common language to explain acceptable use of our Service. Any conflicting sections in a Customer signed service agreement supersede the Terms of Service. Qualtrics reserves the right to disable any User account suspected of violating acceptable use terms. This includes uploading harmful or hateful content (except for valid research purposes), using the Services to “phish” or “spam,” or violating
the Terms of Service or terms of an executed service agreement between Qualtrics and Customer. While Qualtrics cannot prevent Customers from entering any specific type of information, prudence and common sense apply. Research software should not be used to store highly sensitive information, such as bank accounts, credit card numbers, social security numbers, criminal records, or genetic information.

Depending on applicable laws or regulations, it may be necessary for the Customer to de-identify or anonymize sensitive information prior to distributing surveys. Also, it is usually required to receive permission before sensitive information is collected. It is incumbent upon the Customer to know and follow procedures for the legal collection of sensitive information.

DATA PRIVACY

Qualtrics offers general-purpose research services where customers design surveys in an almost infinite number of ways. Since we only provide the platform for the software and Services—and don’t delve into the Customer’s specific implementation—we do not attest or know what Data are entered into our software. We realize that some companies wish to have more specific language regarding data privacy; however, our agreements and this white paper attest to our obligations to safeguard Data and to only process Data for performing the Services.

Being data agnostic is good for Customers, as Qualtrics protects all Data the same, without regard to its meaning or classification. Therefore, it’s impossible for Qualtrics to perform in certain ways based on the classification declared by Customers. All Data are essentially invisible to us.
Certifications / Standards

Qualtrics creates general purpose software products whereby the Customer owns and controls their Data and Users. Therefore, Qualtrics expressly disclaims any knowledge of the Data input to its Services, and cannot classify Data. All Data are considered highly confidential, treated equally, and protected using industry best security practices.

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

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

DATA CENTERS

All Qualtrics hardware (firewalls and servers) and data are located in tier 3 or tier 4 data centers, audited using the industry standard SSAE-16 Service Organization Control 1 (SOC-1) specification. Detailed reports may be requested by existing Customers either from the data center (listed above) or from Qualtrics with a signed confidentiality agreement. More details about data centers are discussed below.

ISO SECURITY STANDARDS

There are many security standards in which an organization may use to safeguard systems and data. Some, like IOS 2700x, were created by the International Organization for Standardization, and specify requirements and best practices for managing company and customer information. Qualtrics adheres to the principles set forth in these standards, including ISO 27001/2.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Qualtrics adheres to the OWASP ASVS methods for development and code review.
FEDRAMP: THE GOLD STANDARD
FedRAMP is considered the “gold standard” for security certifications.

In 2015, Qualtrics contracted with Veris Group to initiate the Federal Risk Authorization and Management Program (FedRAMP) accreditation, thus setting forth a roadmap to achieve one of the highest security ratings in the world.

The partnership with Veris Group provides expert guidance and an independent voice to assess the security posture of Qualtrics, ultimately benefiting its 9,000+ customers. Once Qualtrics is “FedRAMP Ready,” another independent auditor will verify all the security controls written in the submitted documentation.

Presently, Qualtrics is FedRAMP “in Process.” Please visit:

The FedRAMP program was designed to enable U.S. federal agencies to utilize managed Internet-based service providers. The program is designed to comply with the Federal Information Security Management Act of 2002 (FISMA), and is based on the NIST 800-53 Rev. 4 standard with over 900 controls. Many controls may be cross-referenced with such standards as ISO 27001/2, PCI, and HIPAA (Hitech Act).

Security experts recognize that FedRAMP certification means having one of the highest non-military accreditations. It is supported by the Department of Defense, Department of Homeland Security, and GSA. Therefore, these methodologies and procedures will bring leading-edge security to all Qualtrics customers around the globe.

For more information, please visit the following link: http://www.fedramp.com
Human Resource Policies

Qualtrics’ rapid growth requires an influx of great talent. All new hires are held to rigorous standards and high qualifications. Qualtrics also requires background checks and adherence to strict privacy guidelines. Qualtrics is an equal opportunity employer.

CUSTOMER DATA ACCESS POLICY

Upon hire, all Qualtrics employees are required to sign a privacy and confidentiality agreement that specifically addresses the risks of dealing with sensitive information, including Customer accounts and Data. The policy includes the prohibition of access to Data without customer permission. This permission is typically granted for technical support only.

BACKGROUND CHECKS

Qualtrics performs background checks (to the extent permitted by local law) on applicants prior to employment.

PROVISIONING ACCESS

Access to Customer accounts is only given to those with a legitimate business need. This includes members of the Qualtrics support teams (QUni and Client Success), engineering team for specific debugging issues, and select members of our onboarding team that handle creating accounts for new customers. All system and service accesses are logged. No employee has unfettered access to Customer Data. More details below.

SECURITY THROUGHOUT QUALTRICS

Security isn’t just a function of one team, but of the entire organization: engineering, IT, sales, support, HR, and legal departments. Developers are trained in coding best practices. The InfoSec engineers are responsible for securing and monitoring hardware at the data centers. This includes router/firewall configuration, cage security, and reliability verification. TechOps ensures desktop compliance and local server security. Sales and support may receive notice of a customer incident, and are responsible for escalating and investigating. Onboarding/HR staff are responsible for performing background employee checks, and ensuring new hires sign proper paperwork. The Legal team, comprising in-house and outside attorneys and security/privacy staff, ensures a safe work environment and maintains compliance with applicable laws.

Internal security audits are performed continuously via automated systems and verification that written policies are being followed. Qualtrics executives are notified of any abnormalities that would compromise company security or the safeguarding of Customer Data.

SECURITY AWARENESS TRAINING

Qualtrics employees are formally trained each year on company policies and security practices, and more frequently in email. This includes Security Awareness training and quarterly updates. All employees are instructed to immediately report possible security incidents to their manager, supervisor, and company director. The computer security section of the employee manual includes the following topics:
• Privacy law compliance
• Physical security
• Email acceptable use policy
• Access control
• Internet security
• Personal devices in the company
• Information Security Incidents
• Password policy and tips
Network Design, Locations, and Assessments

DATA FLOW AND NETWORK DIAGRAM

In simple terms, transactions involve three parties—the Customer, the Respondents, and Qualtrics Services. The diagram below shows the interaction between these parties.

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

For high availability and speed, base code and static images/docs are stored in the cloud and delivered to Users as efficiently as possible using cache and location information.

Users access the Qualtrics platform with login credentials using a web browser. Customers may choose to authenticate by linking their single sign-on (SSO) system to Qualtrics’ Services. Brand Administrators have full control over Users and the password policy.
QUALTRICS LOCATIONS

Qualtrics is a US-based company with secondary operations in Europe and Australia.

Qualtrics HQ—Headquarters is located in Provo, Utah against the backdrop of 13,000-foot Mount Timpanogos. All U.S. support staff are located here, as well as most salespersons and developers. The new facility officially opened in August 2016 by Governor Gary Herbert. All visitors to headquarters must show a government ID and be escorted. All employees are required to show ID badges upon entering the building.

The 200,000 square foot facility has full electronic access controls, CCTV, and monitored entry points. There is a backup generator in case of power failure. No customer data are stored or processed at headquarters or outside of security data centers, so even if the facility weren’t operational, the software would still continue to function. And since Qualtrics uses ASP/SaaS software for most of its business operations, in the unlikely event of a major catastrophe, temporary offices could be setup in a few days; only power and Internet would be required. The Provo-Orem area is considered low risk for seismic activity, weather, and crime.

Qualtrics US (other locations)—The Seattle office is primarily for development. Dallas and Washington DC are satellite sales offices to accommodate local regions.

Qualtrics EU—Main office is located off Grafton street in the heart of Dublin, Republic of Ireland. It hosts multi-lingual sales and support staff. There are smaller sales offices in London and Munich.

Qualtrics AU—Located in Sydney, Australia. Supports Asia-Pac with sales persons and technical staff. There are small regional offices in Melbourne and Canberra.

DESKTOP POLICIES

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

DATA CENTERS

Qualtrics leases space in two U.S. and one Canadian data centers. They are located in seismically low zones, and in areas least susceptible to mother nature’s whims. Qualtrics owns and operates all server, firewall, and router hardware/software. Outside the U.S., Qualtrics uses co-location data centers with the hardware managed by the data center staff, but with the core operating systems and data always controlled by Qualtrics. Data center personnel have no authorization to access Qualtrics data or underlying software environment (as per contractual agreement and confirmed by SSAE-16 SOC audits).
Equinix — A Tier-4 hosting facility located in Toronto, Canada.
Fortrust — A Tier-3 hosting facility located in Denver, Colorado.
IO Data Center — A Tier-3 hosting facility located in Phoenix, Arizona.
Amazon Web Service Data Centers — These highly secure facilities store Data for specific regions. Locations are Australia and the European Union. AWS provides the secure facility and hardware; it does not process information. All software is operated and controlled by Qualtrics.

Data-at-Rest Location — All Data are stored within the region where the Customer’s primary data center resides, and will not be moved from that region. In other words, if a European customer has its data collected in the EU, its data will be stored and processed in EU. Qualtrics does not transfer data unless requested by the Customer.

Physical Access to Data Centers — Physical access to Data Centers is restricted to a limited number of employees, and includes the locked cage that houses the hardware used to provide the Services. Those employees do not have direct access to Customer Data.
Preventing Unauthorized Access

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

DATA STORAGE

Qualtrics Services use sophisticated databases that logically store Customer Data, as well as organize other components for quick retrieval and faster processing. To best optimize hardware and software, Customers share the same infrastructure, but Data are encoded so that only the correct Data will be sent to the requesting User. Access to Data requires direct ownership (the user who created the survey) or implied access (e.g. Brand Administrator or another User with access). Data at rest are encoded to prevent an unauthorized read access from deciphering the Data. For more advanced encryption, the Qualtrics Data Isolation feature uses AES-256 crypto, and is available for an additional fee.

SUPPORT ACCESS

Only qualified support staff has access to Customer accounts. This includes the QUni, Client Success, and engineering teams. The User must acknowledge the request for account access as shown in the screenshot below. All account access is logged and monitored by the InfoSec team. Each User account shows all login access.

PASSWORD POLICIES FOR THE SERVICES

This section applies to the Qualtrics Services, not the internal company network.

Qualtrics will never ask for any User password. All User passwords are hashed using BCrypt, and thus impossible to decode.

Failed Attempts— In order to block unauthorized access through password guessing, accounts are disabled 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). The Brand Administrator may also re-activate the account.

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. For more complex passwords requirements, SSO integration is recommended.

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 an optional self-service password reset option that sends an email with a link to create a new password.

Single Sign-On—SSO allows Customers to better control user management (additions/deletions) from the Customer’s directory service, directly linked to the Qualtrics authentication service. Industry standard protocols are supported, including LDAP, SAML, OAuth, Token, and Shibboleth.

LOG FILES

Log files contain requestor IP address, protocol, request, result, and other info. Logs are stored on each device, and aggregated and analyzed using various tools. Monitoring systems trigger alarms and actions based on thresholds, thus helping to prevent an attack or other abuse.
Development Practices

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

DEVELOPMENT RELEASE CYCLE

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

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

SECURE DEV WORKSTATIONS

Programmer workstations are Macintosh, and essentially terminals into the programming environment. Extra security is installed on these workstations, including a multi-factor login. This creates a solid operating environment where all code is stored and accessed securely, and access control is assigned to peers or managers for review.

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 staging environment completely separate from the production environment. This testing period eliminates most bugs before they could be introduced to production. No Customer Data are ever used in the testing environment. All code are scanned for vulnerabilities and syntax before deployment.
SEGREGATION OF RESPONSIBILITIES
There are many distinct Qualtrics programming teams, and each team is responsible for specific areas of the code. Engineers may only develop code in their area, and are not allowed to deploy that code to a production environment. This ensures a more secure and reliable development process.

STAGING (TESTING) ENVIRONMENT
All code is deployed and tested in a staging (test) environment that is functionally equivalent to the production environments. No Customer Data are used the staging environment.

DEPLOYMENT AND SECURITY PATCHES
Code is released outside of normal business hours (for a particular region), and with no downtime. If a security vulnerability is found, a fix may be deployed quickly without affecting the Service. Scheduled downtime is not required, although Qualtrics reserves the right to do so. Code is released by the deployment team to each data center on a schedule. All data centers are typically using the same release code within a few days.
Disaster Recovery

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

The purpose of the Disaster Recovery Plan is to ensure prompt and complete return to normalcy in the event of a disaster. The objectives of the plan are to ensure that, in event of disaster: 1) usability is restored promptly with little or no disruption to the User; and 2) Data loss is avoided due to extensive backup measures.

Disaster recovery and business continuity plans are tested bi-annually.

The Recovery Time Objective (RTO) is 24 hours to resume normal operations and Services. The Recovery Point Objective (RPO) is usually less than 4 hours to restore Customer Data. These times are estimates only.

POLICIES PERTAINING TO DRP

- Upon a disaster, Customer Data can be moved to a secure alternate location.
- Recovery processes are mainly automated, with no employee access to specific Customer Data.
- Data security and integrity must be monitored 24x7x365.
- Backup data must be kept in at least one secondary location.

IT DISASTER DECLARATION CRITERIA

In the event of an emergency, priorities include:

- preserving and recovering Data on database servers
- restoring functionality to infrastructure, including firewalls and web server
- restoring support and other operational servers

KEY DOCUMENTS AND PROCEDURES

There are various internal-only security policies that are specific to maintaining services and handling disasters and recovery.
Business Continuity

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

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

GOALS AND OBJECTIVES
The objectives of this plan are to ensure that, in the event of a disaster all necessary support functions of the organization continue without undue delay. Data integrity and availability along with necessary support functions within the organization enable Qualtrics to maintain a trusting relationship with our Customers even in times of disasters.

REMEDIATION
Testing the BC plan is performed at least twice per year. Any significant findings are collected, and a report is produced for Engineering, TechOps, and InfoSec teams to review and create steps necessary to perform the test again and obtain a positive result. The VP of Engineering and Security Officer are also involved in the process.

POLICIES
All business continuity activities are coordinated with input from team leads and managers.

COMMUNICATION
Transparent communication, coupled with complete infrastructure/Systems redundancy, ensure successful continuity in times of disaster.
Backups – Data Retention

This section pertains to Data in the Services, not Qualtrics internal company retention procedures. All respondent Data are backed up by Qualtrics using two methods: automatic propagation across servers (immediate upon collection) and daily complete off-site encrypted backups. However, Customers are encouraged to back up their Data in case of accidental deletion/modification caused by one of their Users, and for their own archive/data retention policies.

AUTOMATIC PROPAGATION

Qualtrics uses advanced data storage technologies that record data to more than one physical device. This process is accomplished as soon as data is written, typically within a few seconds. It protects against storage device failure.

PERIODIC BACKUPS

Qualtrics performs a full daily backup of all production data. These backups are stored at alternate data centers in the same region where the data were created. Every backup file is encrypted using an advanced crypto method with a large key (for security reasons, details are not released).

DATA RETENTION

Since Customers/Users own and control their Data, they are responsible for accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of their Data. They are also responsible for backup (there are numerous download formats and mechanisms) and retaining the backup according to their retention policy. Depending on how active Data were deleted, it may be possible for the User to undelete it using a feature in the software. Once deleted Data are permanently inaccessible, then the User must restore from a personal backup. Survey definitions, response data, and some other data may be easily exported to the user’s own system/device. This is highly recommended as Qualtrics is under no obligation to restore Data not caused by its own negligence.
Incident Response

An incident in this section refers to any discovery of a malfunction of the tool or a deliberate or accidental mishandling of Data (collectively, an “Incident”). Such Incidents require a quick response, and specific employees practice simulated CODE RED alerts. A detailed incident response policy is maintained by the InfoSec and Legal departments.

An Incident includes:

- A malfunction, disruption, or unlawful use of the Service;
- The loss or theft of Data from the Service;
- Attempts (either failed or successful) to gain unauthorized access to Data, information storage, or a computer system; or
- Material delays or the inability to use the Service
- Any event that triggers privacy notification rules, even if such an event is not due to Qualtrics’ actions or inactions.

RESPONSE TEAM

The Qualtrics response team is comprised of members of its support and engineering teams who have expertise in technical issues, network security, and the software. The Engineer-on-call is available for emergency responses 24 hours a day 365 days a year.

NOTIFICATION REQUIREMENTS

An Incident involving personal data (as defined by applicable regulations or laws) may require certain notification procedures. Qualtrics has suitable policies to handle these requests, and has a team of outside attorneys, privacy staff, and security experts to respond to the particular notification needs based on the content disclosed.
Risk Management

This section describes the risk management approach at Qualtrics: the underlying approach, the roles and responsibilities of the board, the senior management team, and other key parties. It also outlines key aspects of the risk management process, and identifies the main reporting procedures.

The following key principles outline Qualtrics’ approach to risk management and policies.

1. The board and senior officers have responsibility for overseeing risk management within the company as a whole.

2. The senior management team supports, advises and implements policies approved by the board and officers.

3. The management recognizes and weighs the financial and non-financial implications of the risks.

4. Managers are responsible for encouraging good risk management practice within their department(s).

5. Key risk indicators will be identified and closely monitored on a regular basis.

RISK MANAGEMENT POLICIES

This broad set of policies encompasses a number of elements that together facilitate an effective and efficient operation, enabling Qualtrics to respond to a variety of operational, financial, and commercial risks. These elements include:

- Policies and procedures
- Monthly reporting
- Business planning and budgeting
- High level risk framework (significant risks only)
- Employee risk frameworks
- Internal audit program
- External audit
- Third party reports

OTHER SECURITY DOCUMENTS

Qualtrics customers with a “need to know” may request these documents provided there is valid reason and an executed confidentiality agreement in place as they contain detailed information about our operations.

Federal Standards White Paper, Security Assessment Questionnaire (SAQ), Standard Information Gathering (SIG) questionnaire, the Detailed Security Assessment, and CAIQ.

For more details regarding Qualtrics security, contact your account executive or Qualtrics support.

//AKM
Privacy Appendix

GENERAL INFORMATION
While Qualtrics agrees to follow applicable laws, most obligations in data privacy laws and regulations are for the data collector/controller. The collector/controller solely determines what data to collect, from whom, and from where. Qualtrics does not view, control or otherwise see the Data and therefore cannot classify, categorize or otherwise differentiate different types of Data. As a data processor, Qualtrics will process and safeguard all data equally without regard to what the data represents. Qualtrics cannot process any specific data differently.

Generally, Qualtrics meets or exceeds data processing requirements for privacy laws worldwide, and adheres to common principles. The full version of this Paper contains appendices specific to privacy laws in the US, EU, Australia, and Canada. Qualtrics has applied for EU-U.S. Privacy Shield accreditation.

RESPONSIBILITIES
The diagram below briefly describes each party’s responsibilities for collecting or processing Data.