qualtrics XM

Cloud Security and Privacy Framework

Information, Security, Privacy, and Compliance

February 2021

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

Terms & Conditions

This document contains confidential information regarding Qualtrics' security related operations and policies. There must be a valid confidentiality agreement signed by your organization and Qualtrics, LLC. This document 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).

You may not disclose any information contained herein to parties that have not signed a confidentiality agreement with Qualtrics.

You may not copy, forward, print, or reproduce this document without Qualtrics' permission.

Overview of Operations

Qualtrics is a Software-as-a-Service (SaaS) who provides a platform for creating and distributing online surveys, performing employee evaluations, web site intercepts, and other research services, referred to as the XM Platform. The XM Platform records response data, performs analysis, and produces reports on the data. All services are online and require no downloadable software. Only modern JavaScript-enabled internet browsers and an internet connection are required. Qualtrics offers multiple products for online data collection: CoreXM, Customer Experience, Employee Experience, Product Experience, Brand Experience, and others. 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.

Definitions

Capitalized terms used in this document are defined below or elsewhere in the document:

“**Account**” means an account specific to an Authorized User, and a collection of Accounts reside under the “**Brand**.”

“**Affiliate**” of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity’s shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.

“**Authorized User**” means any individual to whom Customer grants access authorization to use the Qualtrics platform that is an employee, agent, contractor or representative of (a) Customer; (b) Customer’s Affiliates; or Customer’s and Customer’s Affiliates’ Business Partners. A Brand Administrator is also a User.

“**Brand Administrator**” is the account manager of the Customer account.

“**Business Partner**” means a legal entity that requires use of a Qualtrics platform in connection with Customer’s and its Affiliates’ internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.

“**Customer**” means an organization that has a business relationship with Qualtrics.

“**Data**” means any content, materials, data and information that Authorized Users enter into the production system of the Qualtrics platform or that Customer derives from its use of and stores in the Qualtrics platform (e.g. Customer-specific reports).

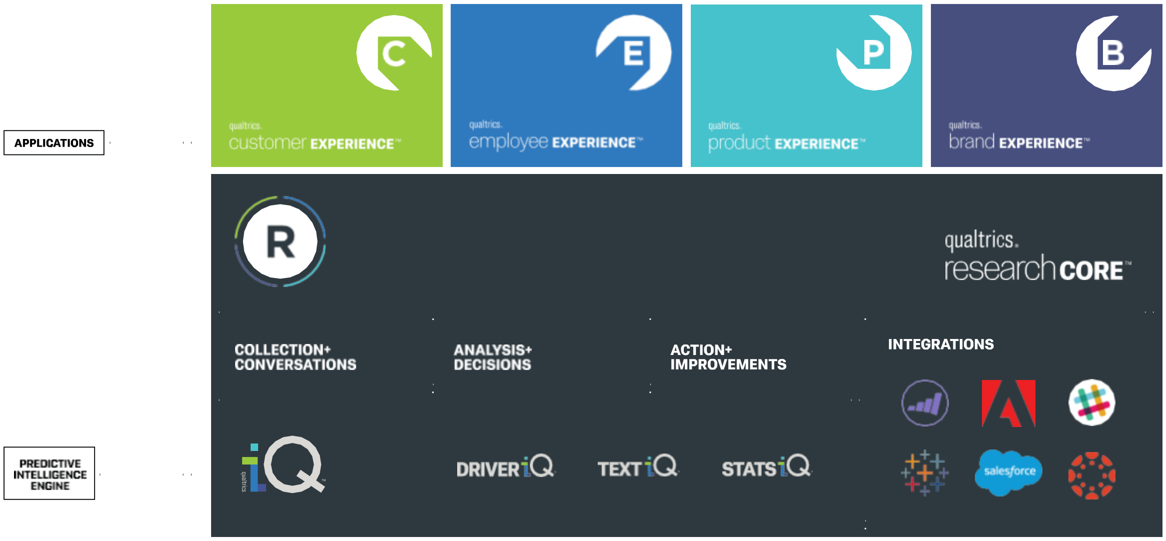
“**QUni**” means Qualtrics University—the technical support department”

“**Respondent**” means an individual who responds to surveys created by a User.

“**Responses**” mean Data collected from surveys taken in web browsers on computer or mobile platforms, or via SMS.

“**Services**” means the range of services provided by Qualtrics, including the software, distributions, support, and online resources.

Service Descriptions


APPLICATIONS
qualtrics. customer EXPERIENCE
qualtrics. employee EXPERIENCE
qualtrics. product EXPERIENCE
qualtrics. brand EXPERIENCE
R
qualtrics. research CORE
COLLECTION+ CONVERSATIONS
ANALYSIS+ DECISIONS
ACTION+ IMPROVEMENTS
INTEGRATIONS
PREDICTIVE INTELLIGENCE ENGINE
iQ
DRIVER iQ
TEXT iQ
STATS iQ
salesforce

PRODUCT NAME	PRODUCT DESCRIPTION
CoreXM	CoreXM is cloud-based software that allows users to collect survey and feedback data, analyze that data, integrate the data with other sources, and report on individual and aggregate responses.
Customer Experience	Customer Experience is cloud-based software that allows users to collect customer feedback, use analytics to predict customer behavior, and deliver customer insights to the organization.
Employee Experience	Employee Experience is cloud-based software that allows users to collect employee data and feedback at each point in the employee lifecycle, use analytics to identify engagement drivers, and distribute reports and insights throughout the company.
Product Experience	Product Experience is cloud-based software that allows users to collect feedback about an organization's existing and prospective products and services
Brand Experience	Brand Experience is cloud-based software that allows users to collect sentiment and perception data about a company's brand.
Research Services	Research OnDemand manages everything for customers -- from designing studies to sourcing respondents, fielding projects, and reporting on the results.
iQ	Qualtrics iQ is a set of advanced intelligent features built directly into the Qualtrics Experience Management Platform. Powered by machine learning and artificial intelligence, iQ makes predictive intelligence and statistical analysis accessible for all users.
DriveriQ	Driver iQ automatically correlates experience data to prioritize the key drivers of customers' business and predict the actions that will drive the most business impact -- all in an easy to read 2x2 matrix.
TextiQ	With artificial intelligence and natural language processing, Text iQ analyzes open text responses so users can see what, in customers' and employees' own words, matters most.
StatsiQ	Stats iQ automatically chooses the right tests and instantly returns results in plain English with powerful visualizations that can be exported to Excel or PowerPoint.

LEGACY PRODUCTS	PRODUCT DESCRIPTION
Research Suite	Research Suite is a previous public name for some of the capability that currently resides in CoreXM, including the ability to collect survey and feedback data, analyze that data, integrate the data with other sources, and report on individual and aggregate responses.
Vocalize	Vocalize is a previous public name for some of the capability that currently resides in Customer Experience, including customer feedback, analytics to predict customer behavior, and reports and integrations to deliver customer insights to the organization
Target Audience	Target Audience is a previous public name for some of the capability that currently resides in iQ Directory, including the ability to maintain contact lists, store response data by respondent, and manage contact frequency.
Site Intercept	Site Intercept is a previous public name for capability on the Qualtrics XM Platform that allows companies to serve website visitors with forms and surveys to provide feedback and other relevant data directly in a website or in an app.
Employee Engagement	Employee Engagement is a previous public name for much of the capability that currently resides in Employee Experience, including collecting employee data and feedback, using analytics to identify engagement drivers, and distributing reports and insights throughout the company.
Qualtrics 360	Qualtrics 360 is a previous public name for a portion of Employee Experience that allows organizations to collect and report on confidential multi-rater feedback of employees.

Locations and Infrastructure

Qualtrics has key operations and data centers in the following locations:

FUNCTION	DESCRIPTION
Production Data Centers	Qualtrics utilizes a combination of both Equinix and Amazon Web Services (AWS) for our production Data storage locations. They are located in the following regions: • United States (East and West) • Canada • EMEA (Germany) • APAC (Australia) Qualtrics utilizes the AWS GovCloud data center for our FedRAMP environment. Data backups and other data elements are stored in Amazon Web Services in the same geographical region.
System Engineering	System Engineering is supported out of the following locations: • United States • Ireland • Poland
Customer Support (QUni)	QUni is supported out of the following locations: • United States • Ireland • Australia

Our production services for our commercial offerings are hosted by third-party data centers that are audited using industry best practices. The infrastructure is located in Equinix data centers is in a dedicated space that is physically separate from other data center tenants. The third-party provides physical and environmental controls, but Qualtrics owns and operates all of the physical infrastructure. The data center providers do not have logical access to Qualtrics infrastructure.

Our FedRAMP environment is hosted by AWS in their GovCloud instance and is audited against FedRAMP.

People

The following teams are responsible for supporting the platform. Their responsibilities may require that they have access to production or develop source code for the environment. Roles include:

ROLE	RESPONSIBILITIES
Qualtrics University (QUni)	• Online / Email / Phone support
Information Security	• Security Alerting and Monitoring • Intrusion Detection • Security Automation • Security Awareness Training • Incident Response
Fleet Engineering	• Physical Hardware Configurations - Server Configurations - Virtualization • Data Center Management • Disk-level Encryption • Capacity Planning
Network Operations	• Network Device Configuration and Management - Configuration Standards - Access Control Lists • Network Access
System Engineers / Quality Engineers	• New Code Development, Hotfixes • Quality Control • Performance Monitoring
Data Engineers	• Database Configuration and Management • Data Backups (availability)
Platform Security	• Define Platform Security Requirements • Vulnerability Management • Penetration Testing • Security Champion Program
IT	• Corporate Infrastructure • Corporate Wireless Networks • Workstation Management
Security Assurance	• Vendor Risk Assessments • Security Compliance (external audits) • Customer Compliance programs
People Operations	• Employee Onboarding / Offboarding • Awareness Training
Legal	• Contracting • Privacy

Policies and Procedures

Qualtrics maintains policies and procedures based upon a variety of security frameworks including: National Institute of Technology Special Publication 800-53 Rev. 4, International Organization for Standardization 27001, and FedRAMP. Control families include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance Media Protection
- Physical and Environment Protection
- Planning
- Personal Security
- Program Management
- Risk Assessment
- System and Services Acquisition
- System and Communications
- Protection System and Information Integrity
- Third-Party Management
- Vulnerability Management

Platform Data

All Data is owned and controlled by Qualtrics' Customers, who are designated as data controllers. Qualtrics is the data processor. All Data is stored and processed in a single multi-tenant data center and in a single region (e.g. EU, US, Canada, APJ) chosen by the Customer. While Data is hostedwithin the region where the Customer's primary data centre resides, Data may be transferred and processed outside the data centre region to comply with Customer requests or instructed (e.g., support purposes, use of subprocessor services) or as strictly necessary to provide the Cloud Service. In all data centers, Qualtrics solely operates and is responsible for all system and developed software.

Qualtrics only processes Data to the extent necessary to provide the software and services and in accordance with our contractual arrangements i.e. to improve products and services, and does not disclose any Data to third parties other than in accordance with applicable law or any contractual agreements.

Customers determine the following about the data stored in the Qualtrics platform:

- Which type of data to collect
- Who to collect data from
- Where to collect data
- What purpose
- When to delete the data

Qualtrics does not classify or represent the Data. All Data is treated as confidential and is processed equally regardless of their meaning or intent.

Control Environment

Executive management has set the tone at the top, which emphasizes the importance of well-designed and operated security controls. Management takes seriously control deficiencies identified in internal and/or external audit reports and takes full responsibility for remediation activities.

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. 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 ASSESSMENT

Qualtrics conducts an annual assessment to identify, manage, and respond to risks to the organization. The assessment process is based on the NIST Framework where threats and vulnerabilities are mapped to different asset classes within the organization.

CONTROL IMPLEMENTATION

Risk treatment plans (i.e., controls) are identified for those risks that fall outside of acceptable levels.
Controls are then evaluated to verify that they are operating as designed.

INTERNAL AND EXTERNAL AUDIT

Internal audits are an important element of maintaining an effective control environment. The program is comprised of several members from various teams, including finance, engineering, security, and legal. At least annually, there is a full review of the effectiveness of all critical internal controls.

As part of Qualtrics Security Assurance programs, external audits provide feedback to appropriate teams on internal controls for key company functions. These are primarily financial and risk based, and separate from security tests. For security tests, see Security Governance section of this document.

REMEDIATION PLANS

Remediation plans are created for audit findings and tracked by the Security Assurance team. The findings are reported up to the Security Governance Committee as part of the monthly meeting. Remediation timelines are consistent with other vulnerability results, namely, critical vulnerabilities within 14 days, high vulnerabilities within 30 days, and moderate vulnerabilities within 90 days.

Monitoring

Qualtrics has implemented a company-wide information security management system to comply with the requirements associated with International Standards Organization, the Federal Risk and Authorization Management Program (FedRAMP) (for the dedicated government environment), and other best practices. This program is monitored by the Security Governance Committee and audited by independent third-party assessors who attest to compliance to these standards.

Information and Communications

Qualtrics maintains internal information security policies and standards to ensure that employees understand their individual roles and responsibilities regarding security, availability, confidentiality, and significant events. The Security Governance Committee is responsible for the overall security of Qualtrics. They coordinate formal and informal training programs, annual security awareness training, the security champion program, and other communication.

An on-call team provides 24/7 monitoring and support to address issues in an efficient manner.

Control Activities

Qualtrics has established a comprehensive set of controls that were designed to meet various security frameworks. Qualtrics has organized these controls in the following domains, with a description of each control in the defined section.

Asset Management

INVENTORY OF ASSETS
Physical inventories of all production systems are documented and maintained for tracking and reporting purposes. A physical inventory of production systems is performed periodically.

ASSET OWNERSHIP
Production systems are assigned a role within the inventory system to document the use and purpose of each device. Each asset has a designated team that owns and maintains the system.

ASSET MOVEMENT
Whenever a production asset is moved from one physical location to another, that move follows the documented change management process. This includes documenting the risk and impact of the move and includes of process of tracking the inventory within the change management ticket. For production disk drives, drives are securely wiped prior to transportation.

BASELINE HARDENING STANDARDS
System configurations are centrally managed via configuration software that automatically updates the configurations on devices. All hardware and operating systems are hardened using industry best methods found in the NIST 800-53 controls. Documented mandatory configuration settings for information technology products employed within the XM Platform system reflect the most restrictive mode consistent with operational requirements. Qualtrics policy requires that information system components be hardened in accordance with CIS Level 1 Benchmarks, where applicable. System configuration settings are updated or reviewed on an annual basis.

TIME SYNCHRONIZATION
Clocks for information processing systems are synchronized with publicly available NTP pool servers. Clocks are synchronized at least hourly.

Business Continuity & Disaster Recovery

BUSINESS CONTINUITY PLAN

Qualtrics has an extensive Business continuity plan (BCP) 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.

- 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 BCP 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 other teams are also involved in the process. 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.

DISASTER RECOVERY PLANS

Qualtrics has an extensive Disaster Recovery Plan (DRP) 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 around building, testing, and responding to disasters. Below is a high-level summary ofactivities:

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 the event of an emergency at off-site or on-site data centers, the IT manager will receive automatic notification via phone and email.
3. Company Directors Notification: If the emergency affects operations, the Qualtrics executive staff will be notified.
4. Relocation of Operations: All systems used to provide the Services are located in secure data centers and are accessed remotely. Alternate data centers provide redundancy in case of a catastrophic data center failure. Internal operations could be temporarily relocated if necessary, and some employees could work from home or shared office.
5. Customer Notification: Customers will be notified by email, telephone, and/or by the web site login page with the details of the emergency. Additional information is located atwww.qualtrics.com/status.

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 backup measures.

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.

EXTERNAL NOTIFICATION PROCEDURES

Customers will be notified by email, telephone, and/or by the web site login page with the details of the emergency. Additional information is located at www.qualtrics.com/status.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN TESTING

Business Continuity and Disaster Recovery plans are tested bi-annually.

Backup Management

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

BACKUP CONFIGURATION

Qualtrics performs a full backup once per week and daily incremental backups of all production data. These backups are stored at alternate data centers in the same region where the data were created. Production backup files are encrypted using Advanced Encryption Standard (AES)-256.

SYSTEM REDUNDANCY

Each of the colocation data centers are designed to be highly available. This includes designing in resiliency and redundancy to minimize the impact of equipment failure and other types of risks. The infrastructure has been designed to eliminate single points of failure. This includes redundant communication lines and power supplies.

Controls around power, climate control, fire detection and suppression are controlled and managed by our co-location provider. These controls are tested annually and documented within an industry accepted report. Our team reviews the reports and visits the data centers regularly to confirm that the controls are operating as designed and tested.

BACKUP DATA RETENTION

As between Qualtrics and its Customers, Customers own and control their Data, and, therefore, Customers are responsible for the 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 own retention policy. This is highly recommended as Qualtrics is under no obligation to restore lost Data not caused by its own negligence. Depending on how active Data is deleted, it may be possible for the User to undelete it using a feature in the software. Once Data is permanently deleted, then the User must restore from a personal backup.

Data backups are retained for 90 days. Restoration from these backup datasets is for disaster recovery only. The backups are electronic (no tape) and stored in an alternate data center in the same region.

Upon termination of a service agreement, Data is retained for a short period of time to allow the Customer to download and archive. After that, Data may be unrecoverable. As stated elsewhere, Data may be deleted by the User at any time using the standard web interface. It is incumbent upon the Customer to determine its own data retention obligations as they relate to their company's policy or legal obligations.

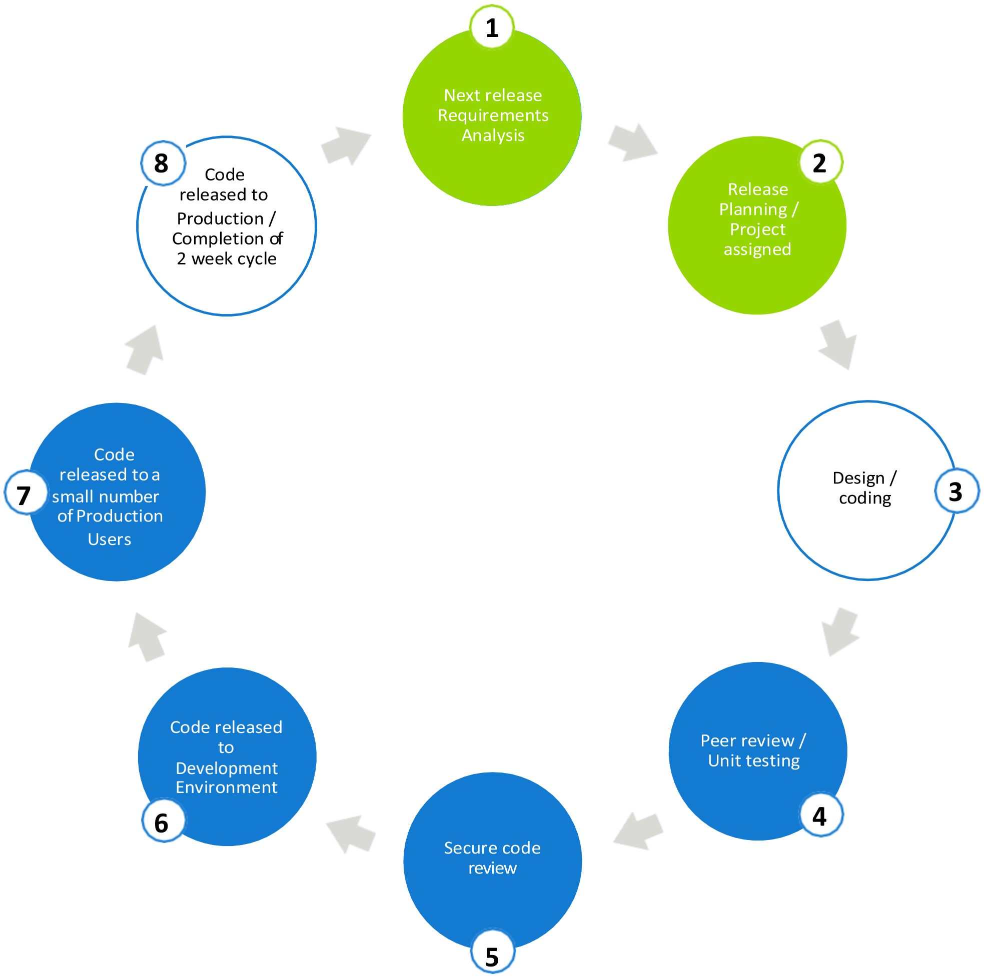
Regarding a request for a litigation hold, because the account is under the Customer's control, it is up to the Brand Administrator to disable User access to the account and prevent Data from being modified. Qualtrics has the ability to disable the entire brand, meaning no Customer access whatsoever. Even so, Qualtrics cannot legally represent anything related to the account usage or Data for litigation purposes.

Change Management

DEVELOPMENT METHODOLOGY

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."


1
Next release Requirements Analysis
2
Release Planning / Project assigned
3
Design / coding
4
Peer review / Unit testing
5
Secure code review
6
Code released to Development Environment
7
Code released to a small number of Production Users
8
Code released to Production / Completion of 2 week cycle

● Planning stages ● Review stages

Figure 1. Development Methodology

CHANGE MANAGEMENT

A formal change management process exists to minimize the impact to the production environment when changes are performed. Changes include source code deployments, upgrades, patching, and security fixes. The change management process requires that all changes be documented, risk assessed, prioritized, planned, tested, approved, and implemented.

Changes are documented within a centralized ticketing system that captures the required data elements. Each change is thoroughly tested before being deployed to ensure a continued stable and operational platform. Thus, we have adopted the following base conditions:

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

APPLICATION CHANGE MANAGEMENT

Staging Environment

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

Code Reviews

Application code review is mandatory for all source code changes. 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. Issues identified in the code review process must be addressed prior to moving to the next step.

Static Code Analysis

As part of the deployment process, source code is processed through a static code analysis tool that checks for potential software bugs and other potential violations of our secure coding practices. If the scan fails, it is sent back to the developer to address the issues identified.

INFRASTRUCTURE CHANGE MANAGEMENT

Routine and periodic hardware maintenance is performed to reduce the impact of performance failures. Changes to infrastructure follows the same change management process as software changes and include documentation that assesses the risk, priority, approval, and implementation of the hardware.

SEGREGATION OF DUTIES

There are many distinct Qualtrics programming teams and each team is responsible for specific areas of the code. Prior to any code deployments, code must go through the peer review process and identified issues must be addressed. Segregation of duties is achieved by ensuring that all code is reviewed and approved by different individuals.

SOURCE CODE MANAGEMENT

Qualtrics uses a source code management tool to enforce version control and code reviews of the source code.

PRODUCT UPDATES

Qualtrics provides information on releases via www.qualtrics.com/product-updates.

Data Management

DATA CLASSIFICATION

Customers own and control all Data entered in or collected by Qualtrics Services. This includes survey definitions, responses, panels, uploaded content such as graphics, and derivative reports/analyses from responses.

Qualtrics does not classify Data entered in or collected by a Customer using the Qualtrics Services.

TYPES OF DATA COLLECTED

There are several data types that surveys collect, and each type generally falls into one of the following categories:

- **Response Data:** Data that survey respondents provide by answering questions in surveys or employee evaluations.
- **Panel Data:** A panel is a respondent list that the Brand can use for the distribution of surveys. This usually includes email addresses paired with a name, but can include additional information. Use of panels is optional.
- **User Information:** The requisite username (User login ID) and password for logging into the platform. All logins are logged, and the Qualtrics User can easily view the log. Usernames are chosen by the Brand Administrator, must be unique for the entire Qualtrics platform, and need not be an email address.
- **Survey Design and Objects:** Surveys created by a Customer along with any graphics and other property uploaded by a Customer and hosted by Qualtrics for use in surveys. Graphics and other objects may be stored in a library.

COMPLIANCE ASSIST

Qualtrics offers Compliance Assist as a tool to help Customers to regulate the collection of personally identified information (PII). The tool can be configured to flag sensitive data requests and redact sensitive data from responses. See https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/ for details.

DATA STORAGE

Qualtrics Services use databases that logically store Data, as well as organize other components for quick retrieval and faster processing. All hardware and software are shared among Customers.

Access to Data requires direct ownership (the user who created the survey) or implied access (e.g. Brand Administrator or another User with access). Response Data is separated by logical controls using the Brand ID as an identifier and verifier. Thus, during each read request, response Data is verified by the ID to ensure accuracy.

While Data is hosted within the region where the Customer’s primary data center resides, it may be transferred and processed outside the data centre region to comply with Customer requests or instructions e.g, support purposes, use of subprocessor services etc, or as strictly necessary to provide the Cloud Service.

ENCRYPTION OF DATA IN TRANSIT

All access to Qualtrics front-end Services is via Hypertext Transfer Protocol Secure (HTTPS) and enforces HTTP Strict Transport Security (HSTS). The platform supports Transport Layer Security (TLS) for all interaction with the platform. Access to the back-end services using the Qualtrics API supports TLS v1.2. Data is processed by application servers and sent to database servers for storage. Respondent Data includes survey questions, graphics, and other content created in the survey design.

ENCRYPTION OF DATA AT REST

Disk level encryption is standard for Data stored on the platform. Data at rest uses AES 256-bit encryption. Unique keys are generated per server or data storage volume.

ENCRYPTION KEY MANAGEMENT

Encryption keys are stored within a software vault where they are encrypted with key encrypting keys of equivalent strength. Keys are rotated whenever data storage volumes are rebuilt.

ENCRYPTED BACKUPS

Data backups are encrypted using AES 256-bit encryption.

EMAIL SECURITY

Qualtrics supports Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Additionally opportunistic TLS is enabled to allow for encryption between email servers.

DATA ISOLATION ENCRYPTION (PREMIUM FEATURE)

As a premium feature, Qualtrics offers the Data Isolation product on the application. Data Isolation is application or database level encryption using AES 256-bit cipher. Data Isolation encrypts response data with a data encrypting key (DEK). The DEK is unique per survey. The DEK is encrypted using a Customer specific master key or key encrypting key (KEK). The KEK is stored in Amazon Web Services' Key Management Service. For additional information, see the Data Isolation Data Sheet.

BRING YOUR OWN KEY (BYOK) (PREMIUM FEATURE)

As part of the data isolation feature, Qualtrics supports BYOK. Use of BYOK requires a customer instance of Amazon Web Services' Key Management Service. For additional information, see the Data Isolation Data Sheet.

DATA USED IN TEST ENVIRONMENTS

Customer data is never used in the test environment.

DATA MODIFICATION

A survey response may be edited if the User is allowed (this is controlled with the survey permissions, “Edit Survey Responses”). This enables the User to correct errors and fulfill certain privacy legislation obligations.

DATA DELETION

Users solely determine when and what Data to delete. Qualtrics provides the platform; Users collect and control their Data. A User with the proper permissions may:

- Delete an individual data point (e.g. city)
- Delete a single response
- Delete multiple responses
- Delete all responses
- Delete the entire survey project (all related data)

These deletion (and modification) options enable the User to fulfill certain privacy legislation obligations.

The Brand Administrator has the ability to undelete Data. This is important, as a User could accidentally or intentionally delete Data. In the same interface, the project data may be undeleted or permanently deleted.

BRAND DELETION

Because customers are in control of their data, Qualtrics encourages Customers to export and delete their data from Qualtrics prior to leaving the platform. At the conclusion of a contract that is not renewed, the Customer is given a short grace period access and delete any data remaining on the platform prior to their access being revoked. After that grace period, the Customer will no longer be able to access any data remaining on the platform. Qualtrics then will delete any remaining data at its earliest convenience, typically after 6 months of inactivity on the brand.

Customers requesting confirmation of data deletion must firstly, perform the deletion of their own data prior to leaving the platform and secondly, make such request 90 days after said data is deleted. Data will persist in backups for 90 days from the date of deletion.

DATA LOSS PREVENTION PROGRAM

Qualtrics has established a program to monitor and alert on unauthorized data moves. Controls include alerting on high risk server commands, monitoring direct database queries, and website filtering on the corporate network.

DISPOSAL OF MEDIA

Formal processes and procedures are in place to securely dispose of devices that may contain Customer Data. These procedures apply to all data center environments. Deprecated or defective media (specifically, hard drives) are erased according to a U.S. Department of Defense compliant 3-pass overwrite standard, and/or physically destroyed.

Endpoint Protection

Qualtrics has policies that describe controls for desktops, servers, and network hardware. These policies are designed from the start to provide the maximum level of security for the intended use of the device.

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. This section applies to the desktops and laptops (collectively, Workstations) used by Qualtrics employees.

OPERATING SYSTEMS

Qualtrics workstations are Apple Macintosh. Qualtrics uses a centralized management solution to enforce device policies that include lockout times, patch management, password strength, and volume encryption. The policy is enforced by user and device, and is stricter with those users that may access customer accounts. No confidential data may be stored on local Workstation drives.

FULL DISK ENCRYPTION

All Workstations require full disk encryption. Native operating system tools are used and are enforced through a centralized management configuration.

APPLICATIONS AND COMPANY DATA

The entire desktop environment is standardized using a secure configuration and basic Macintosh applications as required by job function. This basic setup allows employees to be mobile as users are not necessarily tied to specific devices—though each employee is assigned a device. Internal systems hold some accounting and finance information, but no Customer Data. Instant Messaging is restricted to internal company communications.

Nearly all software used by Qualtrics employees during the normal course of business is SaaS/ASP-based. The rationale for this approach is the same as the one used by Qualtrics salespersons: remote software services are cost effective, reliable, and feature rich.

CLEAN DESK POLICY

A Clean Desk policy has been established to define how data should be viewed on a screen and handled in hard copy form. Any confidential documents in printed form must be securely locked or securely destroyed. Workstation policies define screensaver policies.

MOBILE POLICY

Qualtrics employees own their mobile devices (phone/tablet). If company email will be accessed from that mobile device, there must be a PIN to unlock the device and a timeout (sleep) value of five minutes or less. No Customer Data is accessible from mobile devices.

General Operations

The Qualtrics online privacy statement details how Qualtrics processes personal information that may be collected anytime an individual interacts with Qualtrics. Such interactions include visiting any of our web sites, using the Services, or when calling our sales and support departments etc. A detailed privacy statement is found at the www.qualtrics.com/privacy-statement/. In addition, the Terms of Service (www.qualtrics.com/terms-of-service/) state the terms and conditions, including acceptable use policies, regarding using the Qualtrics Services.

Qualtrics reserves the right to disable any User account suspected of violating our Terms of Service or other policies. 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 order and/or agreement between Qualtrics and Customer (whichever is applicable).

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 sensitive information, such as financial details, credit card numbers, social security numbers, criminal records, or genetic information—unless de-identified. When collecting special categories of data, or sensitive personal data, Customers should only do so in compliance with applicable data protection laws.

CUSTOMER SUPPORT

Qualtrics University (QUni or technical support) staff may ask for personal information before accessing a User’s account to confirm the Users identity. However, they will never ask for a User’s password. Passwords are salted- hashed values and not viewable by any Qualtrics employee. With the User’s permission, QUni may access an account to assist in supporting the User or to diagnose a software problem. Such access may be disabled by the Brand Administrator; doing so may result in decreased support quality.

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 website and services, and to customize the content of our pages for each visitor. In addition, Qualtrics reads browser languages and settings in order to customize surveys for Respondents.

COOKIES

Cookies are used to maintain the session state, and do not include any response Data or personal information. Additional information on cookie usage can be found in our support pages and our Privacy Statement.

ANTI-CORRUPTION AND ANTI-BRIBERY

The Qualtrics organization has been built on transparency and trust, and maintaining solid morals while building a business that started in a basement and has grown to 3,000+ employees. There is a strict anti-bribery/anti-corruption internal policy to conduct all business ethically, not to send or receive bribes, or to otherwise participate in corrupt activities.

BILLING PROCESSES

Qualtrics uses secure third-party services for online credit card payment processing that is PCI compliant. Qualtrics itself does not record or store credit card information.

PROTECTING CHILDREN

Qualtrics does not knowingly collect personal information from children under 13 for marketing purposes. Customers must abide by applicable laws to prevent collecting a child's personal information without parental permission.

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.

INSURANCE

Qualtrics maintains A- or better insurance for industry standard policies and coverages.

Identity and Access Management

Formal policies and procedures have been documented that define the requirements for provisioning and deprovisioning of access to Qualtrics systems. Qualtrics follows the principle of least privilege when assigning access rights to use.

PRODUCTION ACCOUNT PROVISIONING

Access to Customer accounts is only given to those with a legitimate business need and with explicit approval. 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 logins are logged. No employee has unfettered access to Customer Data.

TERMINATIONS: ACCOUNT DE-PROVISIONING

As soon as specific access to systems/services/software is no longer required for job responsibilities, it is revoked. This includes termination of employment as well as changes to roles or responsibilities in the company. The uncoupling process is completed within 24 hours of a role change, or immediately at employment termination. During such an event, a ticket gets created by a manager or HR employee, and emails get sent to various departments. The ticket is managed by HR to ensure that all actions are being performed during the change/termination (such as access to systems and buildings).

Qualtrics uses a centralized password management system to maintain user accounts and passwords to various software/system components. Once access is shut off in this centralized system, the user will no longer have the ability to access production systems.

ACCESS AUTHENTICATION

Access to the production environment is managed through multiple network and authentication layers using multiple usernames, passwords, and multi-factor authentication (MFA) tokens. Prior to accessing the production environment, access to a specific corporate network is required. Access to that network is managed via a username, password, and MFA token. Once connected to the correct corporate network a separate username, password, and MFA key is required to access the production environment through a bastion host. Once connected to the bastion host, an administrator is able to connect to the target system.

Access to our public cloud infrastructure (AWS) requires a username, password, and MFA token to access the management console.

Access to the production infrastructure is restricted to authorized personnel based on job function. Privileged system access is restricted to a limited number of system administrators and their management.

USER ACCESS REVIEWS

Qualtrics performs two levels of access reviews: automated and manual. Access to the corporate network, production environment, and public cloud infrastructure are reviewed nightly via automated scripts to verify that terminated users have been removed.

Logical access is reviewed quarterly by network, server, and information security teams. Reviews are performed to ensure the appropriateness of users.

PASSWORD POLICY

The password policy for privileged accounts on production systems are required to meet the following password parameters:

- Passwords must be a minimum password complexity of 10 characters and must contain a combination of letters, numbers, and symbols based on available system functionality.
- Password maximum lifetime is restricted to 60 days.
- Passwords cannot be reused for at least 16 generations.
- Account lockout settings are enforced after a number of consecutive invalid login attempts and automatically lock the account after the number of unsuccessful attempts is exceeded.
- Passwords are checked against commonly used passwords.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is required to access company applications (e.g. email, internal systems, sales software). Re-authentication is required every 30 days or whenever there is a request to access company applications from another source.

VIRTUAL PRIVATE NETWORK (VPN)

All external access to internal systems is by multi-factor VPN, and limited to employees who truly need such access. It should be noted that this access is for internal systems only, not for access to the data center.

SECRET STORAGE

Secrets (including cryptographic keys and passwords) for the Qualtrics platform are stored in a secure security vault system. Access is restricted based on the principle of least privilege and limited to only authorized personnel. Secrets are rotated periodically.

Incident Response

An incident in this section refers to any discovery of deliberate or accidental mishandling of Data (collectively, an “Incident”). A detailed incident response policy is maintained by the InfoSec and Legal departments.

INCIDENT RESPONSE PLAN

Qualtrics has developed Incident Response policies and procedures to ensure the integrity, confidentiality, and availability of the Data. These policies and procedures are consistent with applicable federal laws, Executive Orders, directives, regulations, standards, and guidance and are set forth by the management teams in compliance with the Incident Response family of controls found in NIST SP 800-53.

An Incident includes:

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

Incident Response Plan includes the following lifecycle steps.

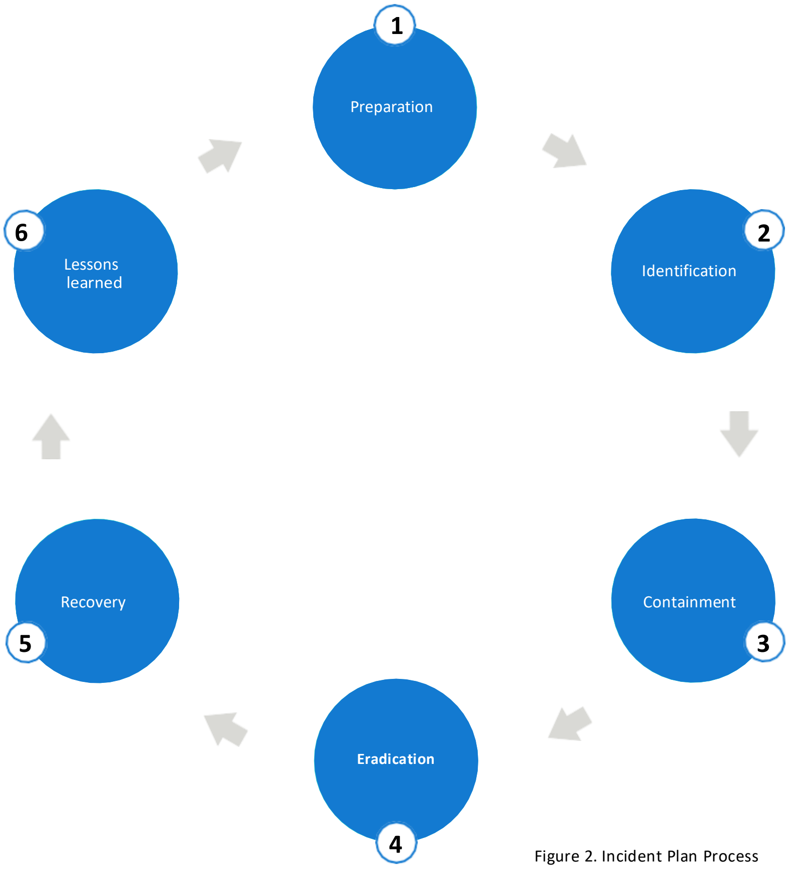


Figure 2. Incident Plan Process

1. Preparation: Build a strong foundation by getting necessary training, acquiring and learning to use tools, and developing policy.
2. Identification: A security event is determined to be a problem. InfoSec reviews IDS, events, and log files; security teams acquire additional data from system administrators and run incident-response tools when necessary.
3. Containment: The team analyzes data to prevent additional systems from being further compromised. InfoSec implements strict firewall rules, checks backup systems, and coordinates with the content provider (if an outside attack).
4. Eradication: Engineering removes malicious components from affected systems or rebuilds them using trusted media and backups.
5. Recovery: Systems are returned to service and monitored for signs of more attacker activity.
6. Lessons Learned: Managers review the security incident, identify its root cause, and assess the incident-handling process to determine what should be improved. It creates an executive summary of the incident and implements process changes.

INCIDENT RESPONSE PLAN TESTING

The incident response plan is tested at least annually and lessons learned are incorporated into the plan. Additionally, as part of the Lessons Learned phase for every incident, the overall plan is evaluated to determine how to improve the overall process.

SECURITY OPERATIONS CENTER PERSONNEL

The Qualtrics response team is comprised of members of its security, support, and engineering teams who have expertise in technical issues, network security, and the software. The Engineer-on-call is available at all times to respond quickly to any issue.

If any Data is affected, the Customer will be notified without undue delay, after a proper assessment, and within two business days. The Brand Administrator is the key point of contact for all notifications, and will be kept aware of the investigation and remediation efforts.

INCIDENT REPORTING CONTACT INFORMATION

If a Security or Privacy Breach/Incident is suspected, contact Qualtrics by email at the following email addresses: privacy@qualtrics.com (legal team) or speak with a support representative at www.qualtrics.com/support/.

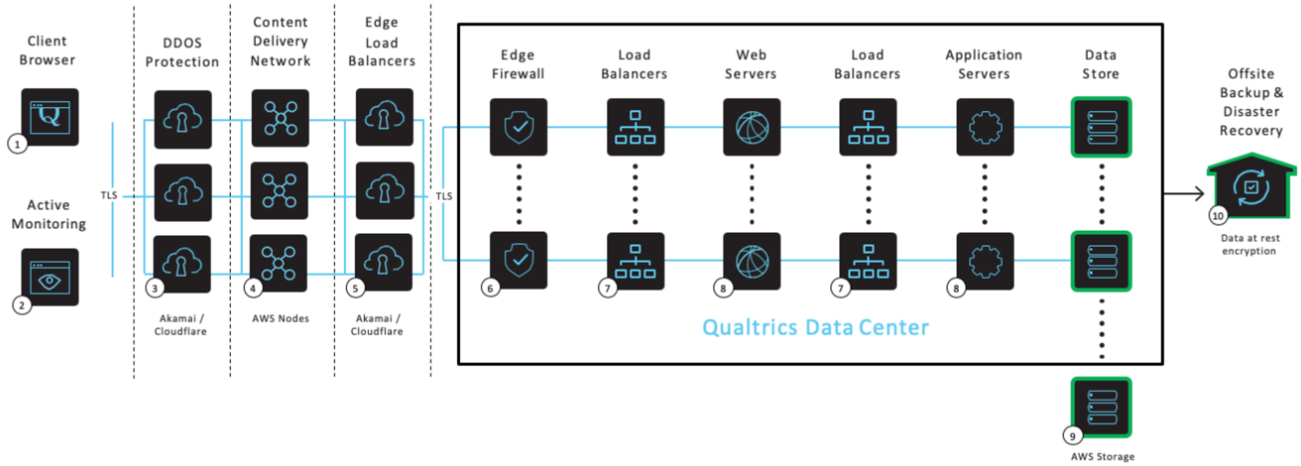
DATA BREACH NOTIFICATION REQUIREMENTS

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.

Network Operations

DATA FLOW

Transactions involve three parties—the Users, the Respondents, and Qualtrics Services. The diagram below shows the interaction between these parties



1 Client Browser – Clients can access Qualtrics from modern browsers without the need for any plugins or other software. Connections are over TLS v1.2 with HSTS

2 Active Monitoring – External monitoring service continually measures availability and performance (including page load times) from multiple locations globally

3 DDOS Protection / Content Delivery Network (CDN) – Security and DDoS protection delivered via Akamai's Cloud Security Suite or Cloudflare (Site Intercept only). Website / App Feedback requests are routed to the nearest edge server in the CDN for a more reliable and higher performing experience

4 Content Delivery Network (CDN) – Qualtrics uses an internally developed CDN that is hosted by AWS. Surveys and respective style sheets are cached in the network to decrease load times for survey takers

5 Edge Load Balancers – Edge load balancers are used to distribute load across our edge firewalls to improve reliability and performance

6 Edge Firewall – All direct access to Qualtrics data centers are further protected via internal hardware firewalls

7 Load Balancers – Load balancers distribute load across web and application servers to improve reliability and performance

8 Web and Application Servers – Web and application servers can be quickly scaled to accommodate demand for Qualtrics applications

9 Data Store – Databases designed for scale and performance for both data collection and reporting. Directory information is stored on database servers in our data centers. Responses are stored in AWS within the same region. Data stores and responses are encrypted using AES-256 with Qualtrics managed keys

10 Offsite Backup & Disaster Recovery (DR) – All data is replicated and backed up offsite (AWS) in an encrypted format. In a DR scenario, a data center is stood up in AWS in order to restore services

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. Email may be configured to use opportunistic TLS to send encrypted messages to an external email server or as a relay to the Customer's email server. Qualtrics leverages a Web Application Firewall to prevent DDoS attacks. The Qualtrics Security Operations Center provides 24/7/365 monitoring of network traffic and responds to DDoS attacks by identifying Botnet traffic.

All access to Qualtrics front-end Services is via HTTPS and enforces HSTS. The platform supports TLS for all interaction with the platform. Access to services using the Qualtrics API supports TLS v1.2. Data is processed by application servers and sent to database servers for storage. Respondent Data includes survey questions, graphics, and other content created in the survey design.

For high availability and speed, base code and static images/docs (no Data) are stored in the content delivery network 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. If SSO is not used, Brand Administrators have full control over Users and the password policy.

WEB APPLICATION FIREWALL

Qualtrics takes a multi-tier approach to protect systems that host the Services and Data. Qualtrics employs a web application firewall for protection against DDoS and web application attacks. Any detected attack—including application-layer DDoS, SQL injection and XSS—will be thwarted, and traffic will be dropped or rerouted, so downtime is minimal.

NETWORK POLICY ENFORCEMENT POINTS

Tools and processes have been implemented to monitor and control communications at the boundary of the production environment. Web applications firewalls and border routers are configured to filter potentially harmful network traffic.

Access control lists are applied to border devices to enforce a "deny all, but allow by exception" policy. Load balancers are used to manage connections within the production environment. Firewalls with IDS/IPS capabilities are enabled.

NETWORK SEGMENTATION

Qualtrics systems consist of three logically and physically separate networks: corporate, development / test, and production networks. The corporate network supports internal business functions and the authentication mechanism is completely separate from the development / test and production environments.

The development / test network is designed to support software development and quality engineering. No wireless networks are attached to this network.

The production network is located in one of the co-location data centers and is designed and built to be fully redundant. Network infrastructure is designed to be fully redundant and fault tolerant. Servers are configured with redundant network interface cards and power supplies. No wireless networks are attached to this network.

WIRELESS NETWORKS

Wireless networks are located on the corporate network. All wireless networks are encrypted, with WPA2, and require MFA. Qualtrics uses devices to detect and neutralize wireless threats, delivering state of the art protection to the most security conscious distributed networks.

People Operations

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

BACKGROUND SCREENING

To the extent permitted by local law, employment offers at Qualtrics are extended contingent upon satisfactory completion of a background check. Background checks may include verification of any information on the offeree's resume or application form, including the items on the below chart.

	EUROPE	AUSTRALIA	UNITED STATES
Education Verification	●	●	●
Employment Verification	●	●	●
Criminal Check (where allowed by law)	●	●	●
SSN Trace			●
Extended Global Sanctions			●
DOJ Sex Offender			●
Locator Select and Verification			●

EMPLOYEE AGREEMENTS

Upon hire, all Qualtrics employees are required to sign an employment agreement containing privacy and confidentiality obligations that specifically address the risks of dealing with confidential information, including Customer accounts and Data. The policy includes the prohibition of access to Data without User permission—typically granted for technical support only. Any employee found to have violated this policy will face internal disciplinary action, with possible legal consequences.

DISCIPLINARY PROCESS

Employees alleged to have violated Qualtrics information security policies are investigated. Depending on the severity of the allegations and results of the investigation, Qualtrics may suspend the employee's access to the affected systems. Following the investigation, notification occurs to the appropriate internal parties regarding results of the investigation and any disciplinary actionstaken.

Security Governance

INFORMATION SECURITY MANAGEMENT SYSTEM

The Information Security Management System (ISMS) defines the overall security function at Qualtrics. The ISMS includes policies, procedures, and standards that define the controls that help support the confidentiality, integrity, and availability of the XM Platform. Additionally, the ISMS outlines the roles and responsibilities of employees at Qualtrics to help protect the confidentiality, integrity, and availability of the platform.

SECURITY GOVERNANCE COMMITTEE

The Security Governance Committee (SGC) oversees the Information Security Management System. It is made up of Technical Operations, Legal, and InfoSec members. The SGC convenes monthly to discuss current issues, status on security-specific engineering projects, and updates on certifications. The SGC responsibilities include:

- Oversees security policies and procedures, including creation and updates Overseeing
- security risk assessments and audits
- Monitoring compliance with the Information Security Management System

SECURITY CERTIFICATIONS

In order to demonstrate Qualtrics' commitment to Information Security, they have implemented a Security Assurance program to obtain and maintain security certifications. Qualtrics has the following securitycertifications:

SOC2 Type II

Security, Confidentiality, Availability

ISO 27001

Security Management Controls

FedRAMP

Government Data Standards (Moderate)

CYBER ESSENTIALS

Cyber Threat Protection

HITRUST

CSF v9.3

FIPS SECURITY REQUIREMENTS

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

Site Operations

Qualtrics is responsible for the physical security controls at the Corporate offices, and components of physical security controls within the co-location data centers. Physical security controls of the colocation data center are the responsibility of the data center service provider. The controls are monitored annually through onsite visits and the review of third-party audit reports.

Corporate Offices

SECURED FACILITY

Physical access to the facility and computer equipment located at corporate facilities is managed through the use of badge readers at all entry and exit points. The badge system is configured to log all card swipes. The badge system is configured to alert if doors are forced or if doors are held open for an extended period of time. Video surveillance is recorded and maintained for a minimum of 30 days to allow for a review.

VISITOR ACCESS

Visitor access is logged at the corporate facilities. Visitors must be escorted at all times. Visitors must sign-in prior to accessing any corporate facility.

Qualtrics Responsibilities (Data Centers)

DATA CENTERS

Qualtrics leases space in five colocation data centers. Qualtrics owns and operates all server and network devices. Data center personnel have no authorization to access Data or the underlying software environment (as per contractual agreement and confirmed by independent audits).

In general, all data centers utilized by Qualtrics:

- are in non-descript buildings
- access controls to all areas (including loading dock) using biometrics and card
- readers log and monitor all entry and exit access
- have 24/7 on-site guards
- constantly monitor power, fire, flood, temperature, and
- humidity geographically diverse

Data centers are audited using industry best practices. Detailed reports may be requested by existing Customers either from Qualtrics with a signed confidentiality agreement.

PROVISIONING PHYSICAL ACCESS

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 Data. Access to the data center is managed by Technical Operations. They are responsible for provisioning and de-provisioning physical access.

PERIODIC REVIEW OF PHYSICAL ACCESS

Physical access reviews of Qualtrics personnel with access to the data center are performed quarterly.

Systems Monitoring

Various tools are used to monitor the confidentiality, integrity, availability, and performance of the production environment, such as intrusion detection systems, performance and health systems, and security event correlation systems.

SECURITY MONITORING
The platform is monitored for security breaches, system performance, and other key performance indicators. Service teams have configured production servers, databases, and network devices to report their logs into a Security Information and Event Management (SIEM) system. The production systems are configured to capture log events including: logon events, account management events, privilege functions, and other system events. The SIEM is configured to monitor and alert when certain thresholds and activities are performed.

Alert notifications are monitored by the Security Operations Center (SOC) and service teams. Alerts are acknowledged and corrective action is taken as needed. Documented procedures are followed to address security breaches, incidents, and service disruptions. Automated monitoring systems are supplemented with manual reviews of system logs and physical access logs.

INTRUSION DETECTION
Host-based intrusion detection has been implemented on all servers in all data centers. Host-based intrusion detection is monitoring key system directories for changes and other evidence of compromise.

PERFORMANCE MONITORING
Personnel in offices worldwide support the continuous operations of the platform. The environment is monitored 24/7 for reliability and performance. Monitoring is performed through a variety of automated and manual processes.

Customer impacting performance incidents are tracked within an online ticketing system. Each incident is assigned a priority based on the impact of the event. In most cases, a representative from each service team joins a conference bridge to help analyze, contain, and resolve the issues as quickly as possible. As the incident is triaged, teams that are responsible for the incident work to resolve the problem. After the incident has been resolved, those teams investigate and document the root cause of the incident and how it can be prevented in the future. The root cause analysis is then presented to key personnel and lessons learned are incorporated into key business processes.

Customers can monitor system performance at the following URL: www.qualtrics.com/status.

System availability and performance reports are discussed during monthly leadership meetings. System capacity for strategic growth and performance is monitored on an ongoing basis.

LOG RETENTION & PROTECTION

System and performance logs are sent to a SIEM for long term storage. The SIEM is configured to “Write Once, Read Many” to prevent logs from tampering. Log files typically contain requestor IP address, protocol, request, result, and other info. Real-time dashboards provide insight into the log files using advanced analysis techniques. No personal data is captured in log files, and they are internal only and unavailable to Customers.

Active (live) logs are retained for at least 90 days and may be used for incident responses. Archive logs are retained for one year in compressed form for possible future forensic purposes.

Third Party Management

THIRD PARTY DUE DILIGENCE

To help mitigate risk to Qualtrics and our customers, the Security Assurance and Legal teams performs regular reviews of suppliers and the services they provide. The Supplier Risk Assessment process evaluates suppliers based on an internal and external risk score. The internal risk score is based on types of data that will be stored, where the data will be stored, and how it would be accessed. The external risk score is calculated based on responses and evidence provided by the supplier. Control areas reviewed include but are not limited to: information security, logical access, physical security, vulnerability management, change management, data security, and data privacy.

ANNUAL THIRD-PARTY ASSURANCE REPORT REVIEW

Key suppliers are evaluated annually for ongoing compliance with key processes and contractual obligations to achieve availability, confidentiality, and security and privacy commitments. Data centers must have a third-party assessment / audit to validate that physical and environment controls are in place and operating as designed. In addition to these audits, Qualtrics personnel visit those data centers where company owned assets are located. Controls that are evaluated for data centers consist of the following:

Environmental Safeguard controls (e.g., Heating Ventilation and Air Conditioning (HVAC), UPS, etc.) and Physical Security controls (e.g., CCTV, access systems, etc.)

THIRD PARTY AGREEMENTS

The Qualtrics Legal team ensures information security requirements are captured as part of service level agreements with new suppliers. In cases where a supplier's risk assessment results in a higher risk, additional monitoring areas may be required, including follow-up from the Qualtrics Security Assurance team. Third party service providers who may have physical or logical access to the Qualtrics platform are required to acknowledge and agree to confidentiality requirements.

Training and Awareness

GENERAL SECURITY AND PRIVACY AWARENESS TRAINING

Qualtrics employees are formally trained on company policies and security practices. This training occurs at the time of hire and at least annually through in-person or online for remote employees. In addition to the in-person trainings, regular updates are provided throughout the year through email, intranet postings, and regular company meetings. All employees are instructed to immediately report possible security incidents to their manager, InfoSec, and Legal. The employee handbook includes policies and guidance on 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
- Insider threat

SECURITY TRAINING FOR ENGINEERS

System engineers receive additional training throughout the year via regular team meetings and other online learning activities. Training topics include:

- OWASP Top 10 Vulnerability Training Secure
- Development Best Practices
- Training on security tools (e.g., static code scanning, etc.)

Vulnerability Management

VULNERABILITY ASSESSMENT, TRIAGE, AND RESOLUTION

Qualtrics has a robust vulnerability management program which includes using multiple methods to identify vulnerabilities in the environment. These methods include anti-malware software, internal and external penetration tests, vulnerability scans, and source code scans. If a vulnerability is detected, it is assigned a ticket and a rating: critical, high, medium, or low. High-rated vulnerabilities are evaluated for a) likelihood of exploitation, b) impact if exploited, and c) time to test and deploy.

Remediation plans are developed as necessary to address high risk vulnerabilities within 30 days and moderate risk vulnerabilities within 90 days—except in extenuating circumstances.

ANTI-MALWARE PROTECTION

Anti-malware (anti-virus) software is loaded on the front-end firewall systems. All incoming packets are checked in real-time. Suspected malware is quarantined and prevented from being downloaded to workstations. Definitions are installed automatically.

Anti-malware software is installed on end-user workstations. Definitions are updated daily and scans are run whenever a file is written or read (i.e. active scanning). If malware is detected, it is quarantined and an alert is sent to the Qualtrics InfoSec team and an investigation is triggered.

PATCH MANAGEMENT

Patch management is performed whenever a new core set of software is to be deployed. Patches are fully tested and deployed as soon as practical, based on their impact. Systems which require patching are typically detected as part of vulnerability scans, however, Qualtrics Engineering team members also subscribe to security advisories for the technologies used and will receive notification when patches are released.

PENETRATION TESTING

External security assessments are performed by an independent third-party. Penetration tests against the production environment are performed annually. Remediation plans are documented to address findings from the report. Findings and remediation plans are presented to the Security Governance Committee and tracked until they've been addressed.

Qualtrics maintains an internal penetration team that is continuously testing elements of the applications looking for bugs. Similar to external tests, findings are presented to the Security Governance Committee for their review.

VULNERABILITY SCANS

External vulnerability scans are run nightly against the environment. Internal vulnerability scans are run weekly. Vulnerability scanning tools are configured to update their definition regularly and scans the environment to identify missing patches and other misconfigurations. Patches are applied based on the overall risk rating.

Using the Service

This section is specific to Customers and their Users using the Qualtrics platform—the products and Services.

BRAND ROLES

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

- **User:** A person that has access to the platform for creating and distributing surveys, as well as viewing and analyzing data, as allowed by the role permissions. Multiple User roles may be created with varied permissions.
- **Brand Administrator:** A Brand is an account with one or more Users. A Brand Administrator has permissions to login as any user within the Brand, as well as restrict the permissions of any other User in the Brand. Brand Administrators also have access to other administrative tools, such as a password reset function. This role is assigned by the Qualtrics onboarding team, and thereafter all Brand control is under the full control of the Brand Administrator.
- **Division Administrator:** Has all the same access as Brand Administrators, but only within a Division, an administrative level organization that is a subordinate of the Brand. Divisions can be established by a Brand Administrator.
- **API Token:** The REST API requires a token that is used to authenticate prior to communication with the API service. A User with appropriate rights may generate a token (a long string of random digits) as often as desired.

ACCOUNT ACCESS CONTROL FOR THE SERVICE

- **The Qualtrics user who owns the survey:** This is the person who creates the survey. Ownership of a survey can also be transferred by a Brand Administrator. Login access is recorded for each user account.
- **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 them. A Division may contain a collection of Groups and Users, with a Division Administrator.
- **Collaboration:** Individual surveys may be collaborated (or shared) with other Users or Groups. When collaborating, a User can specify which permissions other Users or Group Members should have, including access to view associated Data. Access to collaboration functions may be restricted on a per-User basis. Also, survey distribution may be restricted until approved by a designated user.
- **Brand Administrator:** The Brand Administrator has full control over the Brand, and may log in to any User account within the Brand (the audit log will show that login).

An approval process can be leveraged to ensure that surveys are reviewed and approved prior to distribution. This will help prevent a rogue User from sending out a survey without a formal process or other consent.

PASSWORD POLICIES FOR THE SERVICES

This section applies to password policies available in the Qualtrics platform that, like other functions, are solely under the control of the Brand Administrator.

Qualtrics will never ask for a User password. All User passwords are hashed. Password settings available within the platform include:

- **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 login attempt is performed). The Brand Administrator may also reactivate the account.
- **Password Complexity:** Settings for length, complexity (non-alpha characters), and periodic password expiration are available at the Brand level. For more complex password requirements, SSO integration is recommended. A unique error message may be sent when a password doesn't meet the stated requirements.
- **Password Expiration:** Settings for expiration are defined within the organization settings. The configuration is defined in number of days. A unique error message may be sent when a password doesn't meet the stated requirements.
- **Forgotten Password Policy:** If a user forgets their password or makes 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, CAS (Central Authentication Service), Google OAuth 2.0, Token, Facebook, and Shibboleth (SAML).

These settings are controlled within the Advance Security Tab.
See https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/ for more details.

SURVEY SECURITY AND USAGE

There are several ways to protect surveys from being "stuffed," or from 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.

Brand Administrators control the brand, including authenticated users, survey design, distribution, and collected Data. There is an option to require approval before a survey is distributed, thereby enabling a manager (or other designated User) to review before the survey is sent. Qualtrics is not responsible for any Data lost or stolen due to negligent Users.

PRIVACY IMPACT ASSESSMENT

Since Qualtrics products are self-service, Customers have shared responsibilities regarding the security and use of the Services. Each Customer may conduct a Privacy Impact Assessment (PIA) based on their specific use of the platform and information to be collected. All data elements (survey definition, responses, reports, distribution, approvals) are the responsibility of the User and/or the Brand administrator. Creating and managing Users rests solely upon the Brand Administrator, and only those persons who need to use Qualtrics should be given access. Customers may choose to use Single Sign on (SAML) for full control over which Users have access to the Qualtrics platform.

Qualtrics has performed its own PIA based upon the NIST 800-53 standard. The report is internal only.

User Controls

The Qualtrics platform is designed to be a self-service platform and as such, there are a number of controls that Qualtrics' Customers should implement to support their compliance programs. When a Customer's audit function reviews the security of the Qualtrics platform, they will need to work with their Brand Administrator to review the following controls:

USER CONTROLS

Password Settings: The platform allows for two types of authentication to the platform: 1) Local Accounts and 2) Single-Sign On (SSO). For local accounts, password settings are configurable within the Security tab. (https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/)

For SSO, password settings would be located in the customer's Identity and Access Management tool.

Session Timeouts: Customers that have access to the Security tab have the ability to configure session timeout limits. (https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/)

Multi-factor authentication: Customers that have access to the Security tab have the ability to configured Multi- factor authentication (MFA). (https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/)

Audit Logs: The platform allows for audit logs to be pulled from the system via a default API call to the platform. Information on how to get activity logs are is located on the Qualtrics API page. (https://api.qualtrics.com/docs/get-activity-log)

User Provisioning/Deprovisioning: Customers are responsible for creating valid user accounts within the application. Qualtrics creates an initial customer administrator account (i.e. Brand Administrator), but the Brand Administrator manages any additional account creation and management.

User Access Reviews: Customers are responsible for managing access within the application, including the performance of a periodic user access review.

Data Retention: Customers are responsible for defining data retention requirements and enforcing them within the application.

Data Backups: Customers are responsible for performing data backups and retaining the backups according to their data retention policies.

Geographic Restrictions: Customers are responsible for determining if geographic restrictions are required for the storage and accessing of data within the platform.

Authentication Whitelists: Customers can set up the application to limit which IP addresses are allowed to access their instance. Customers are responsible for maintaining this list.

NOTE: SSO is required for this control.

Data Storage: Customers are responsible for selecting which data center where their data will be stored.

Data Labeling Requirements: Customers are responsible for labeling data that is stored within the platform. Additionally,data that is exported from the platform will need to be labeled.

Data Deletion: Customers are data owners and are therefore responsible for deleting the data from the platform. Export options are available at the following URLs:

- Inside the Platform: https://www.qualtrics.com/support/survey-platform/data-and-analysis-module/data/download-data/export-options/
- API - api.qualtrics.com

The data will then reside in Qualtrics backups for 90 days.

Incident Response Plan: Customers are responsible for developing their own incident response plan.

Data Quality: Customers are responsible for reviewing and evaluating the quality of the data within the platform.

Compliance Assist: Customers are responsible for enabling and defining PII elements that should not be collected as part of a question or in the response.

Appendix A: US Privacy Regulations

HEALTH INSURANCE PORTABILITY AND ACCESSIBILITY ACT (HIPAA)

All Data is considered confidential without regard to classification, purpose, meaning, or specific designation (such as Protected Health Information (PHI), ePHI, PII, or publicly available).

Related to HIPAA, the HITECH (Health Information Technology for Economic and Clinical Health Act) have updated assessment rules to ensure that electronic data is properly protected and best security practices followed. By using secure and certified data centers, Qualtrics ensures the highest protection per HITECH requirements, and meets or exceeds the general requirements in the Security and Privacy Rules. Qualtrics has completed a HIPAA self-assessment and attests that it meets or exceeds the Security and Privacy Rules as related to a Business Associate.

Customers must monitor their Users and Data, and enforce their own policies regarding HIPAA requirements. Qualtrics does not control the account Users, who create and administer surveys, or others who might have access to respondent data once downloaded from the Services.

A Business Associate Agreement (BAA) will only be considered when the customer is a covered entity or business associate. As a BA, Qualtrics may take on extra legal obligations even though it cannot confirm the details of data collected or exercise control over Users. Destruction of PHI, similar to all other Data, must be performed by the User when that Data is no longer required. Language must be included in a BAA to cover the particular nature of our self-service, data-agnostic business model.

If a government authority requests access to Qualtrics records or Data, Qualtrics will contact the Customer where permitted by applicable law.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 C.F.R. Part 99 (FERPA) relates to the privacy, access, and disclosure of student information. The Act specifies certain restrictions and disclosure procedures regarding student information. Qualtrics will not disclose or use any Customer information, except to perform the Services unless required by applicable law or in accordance with contractual agreements. If law enforcement requests or a court order is served, Qualtrics will, to the best of its ability, notify the customer before any information is released. Because Customers own and control their Data, Qualtrics cannot respond to individual requests related to student information.

Qualtrics conforms to the intent of the Act if the Customer agrees to be responsible as data owner, as stated in this summary: FERPA regulations require a state or local educational authority to use “reasonable methods” to ensure “to the greatest extent practicable” that any entity designated as its authorized representative to receive data to conduct evaluations, audits, or compliance activities (1) uses student data only for authorized evaluation, audit, or other compliance purposes; (2) protects the data from further disclosure or other uses; and (3) destroys the data when no longer needed for the authorized purpose.

Appendix B: EU Privacy Regulations

GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) came into effect on May 25, 2018. The GDPR is a comprehensive data protection law that regulates the use of personal data by organisations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where the organization is located. and provides individuals rights to exercise control over their data..

Qualtrics enables its Customers to be GDPR compliant by providing the necessary documents and tools to fulfill its obligations as a data controller. Several sections in this paper describe the tools (authentication and access; response editing and deletion).

Briefly stated, Qualtrics meets its obligations as a data processor by meeting the following key, though not exhaustive, GDPR obligations:

- provide sufficient guarantees to the controller to implement appropriate technical and organizational measures designed to safeguard all Data
- process Data (that could include personal data) to fulfil its obligations as related to the Services and applicable agreements
- enable Users to modify and delete individual data points
- enable Users to modify and delete complete survey responses
- enable Users to modify and delete the entire project (responses and survey definitions)
- provide security-related documentation that describes the processes and procedures for safeguarding the Data (certain documents subject to the execution of confidentiality agreements)

As stated elsewhere, Qualtrics processes all Data the same regardless of its intent or meaningand protects Data using industry-standard security practices.

GDPR Article 28, Section 3, requires that a contract be in place between a data controller and a data processor to govern the processing of personal data. The Qualtrics Data Processing Agreement is available upon request, or can be signed electronically at https://www.qualtrics.com/gdpr/.

RESPONSIBLE PARTIES

Both Qualtrics and its Customers (controllers) are responsible for compliance with GDPR, in Qualtrics case as a data processor, and in Customer's case as a data controller.

EU-US PRIVACY SHIELD / SWISS-US PRIVACY SHIELD

While Qualtrics is certified under the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield, Qualtrics no longer relies on Privacy Shield for transfers of Data to the US. For more details about the Privacy Shield program, please visit https://www.privacyshield.gov/.

Qualtrics complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union (EU), the United Kingdom, and Switzerland to the United States, respectively, including the onward transfer liability provisions. Qualtrics received original self-certification in the Privacy Shield program by the U.S. department of commerce in December 2016. Qualtrics continues to renew its certification where such framework is available and can be used as a valid transfer mechanism.

PRIVACY SHIELD REQUIREMENT	RESPONSIBILITY OWNER
Individuals have the right to opt-out of having their PII collected	Customer
Require an individual to opt-in when sensitive data is collected	Customer
Must have contracts with third parties to protect PII transferred to them	Shared
Must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction.	Shared
Only process PII for the stated purpose of research as long as such data is stored	Qualtrics
Individuals have the right to access their personal info	Customer
Individuals have recourse mechanisms	Shared
Adherence to other local laws	Shared

A compliant privacy policy is posted at http://www.qualtrics.com/privacy. Qualtrics retains the American Arbitration Association/International Centre for Dispute Resolution should a dispute arise. Qualtrics is fully committed to Privacy Shield.

Considering the nature of the Services, Qualtrics must inform its customers about:

- its participation in the Privacy Shield
- the types of personal data collected and potential entities or subsidiaries of the organization also adhering to the Principles
- the purposes for which it collects and uses personal information about them
- how to contact the organization with any inquiries or complaints
- third parties to which it discloses personal information, and the purposes for which it does so
- the right of individuals to access their personal data
- the choices and means the organization offers individuals for limiting the use and disclosure of their personal data
- the possibility, under certain conditions, for the individual to invoke binding arbitration
- the requirement to disclose personal information in response to lawful requests by public authorities

Note: this is not an all-inclusive list

Appendix C: Australian Regulations

AUSTRALIA FEDERAL PRIVACY ACT

The Privacy Act 1988 (Cth) applies to Federal Government agencies and to private organizations that:

- handle personal (including health and other sensitive information); and
- carry on business in Australia; and
- have an annual turnover of more than AUD $3 million or is related to a company that does (APP Entities).

The Privacy Act includes 13 Australian Privacy Principles (APPs) that set out binding standards and obligations APP Entities must meet the rights of individuals in relation to handling, holding, accessing, collecting, using, disclosing, storing and correcting personal information.

As a principles-based law, the Privacy Act provides APP Entities with a degree of flexibility and allows them to adapt their information handling to the needs of their business. This allows APP Entities to operate without undue restrictions. Each APP Entity (the Qualtrics Customer) needs to consider how the principles apply to its own situation.

Qualtrics generally meets or exceeds the APPs that relate to its processing of Data—specifically, only using Data to fulfil its obligations as related to the Services and applicable agreements, maintaining a high level of security, and having a transparent privacy policy.

AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUALS

The Australian Department of Defense provides an Information Security Manual (ISM) on which Federal agencies as well as state and local government agencies base their own ISMs. Key principles and controls outlined in the ISM align with FedRAMP and ISO 27001 to which Qualtrics has attained formal accreditation (see “Certifications / Standards”).

Qualtrics’ Australian operations were designed to facilitate physical storage of information with a ‘handle-as’ classification PROTECTED or below. This includes UNCLASSIFIED DLM. Many of Qualtrics’ Australian Government customers conduct periodic threat/risk assessments (TRAs) on Qualtrics’ processes and procedures.

The Australian Signals Directorate (ASD) maintains an Information Security Registered Assessors Program (IRAP) which endorses security professionals to conduct security assessments in line with the Cloud Security Guidance.

Appendix D: Canadian Privacy Regulations

PRIVACY ACT OF 1983

This Act sets rules and obligations for the Canadian federal agencies and departments to limit the use of personal information. Any Canadian agency that uses Qualtrics products to collect personal information must comply with this Act.

PIPEDA: PERSONAL INFORMATION PROTECTION AND ELECTRONICS DOCUMENTS ACT OF 2000

Canada's comprehensive national private sector privacy legislation is known as PIPEDA. The goals of the Act are to create trust in electronic commerce transactions and to establish a level playing field so the same rules apply to all businesses.

It should be noted that Canadian provinces may have their own privacy laws, and if they are equal to or stronger than PIPEDA, then they take precedence.

PIPEDA has ten Fair Information Principles, listed below. Qualtrics has completed a self-certification of the Principles.

- **Accountability:** Organizations should appoint someone to be responsible for privacy issues. They should make information about their privacy policies and procedures available to customers.
- **Identifying purposes:** Organization must identify the reasons for collecting your personal information before or at the time of collection.
- **Consent:** Organizations should clearly inform you of the purposes for the collection, use or disclosure of personal information.
- **Limiting collection:** Organizations should limit the amount and type of the information gathered to what is necessary.
- **Limiting use, disclosure and retention:** In general, organizations should use or disclose your personal information only for the purpose for which it was collected, unless you consent. They should keep your personal information only as long as necessary.
- **Accuracy:** Organizations should keep your personal information as accurate, complete and up to date as necessary.
- **Safeguards:** Organizations need to protect your personal information against loss or theft by using appropriate security safeguards.
- **Openness:** An organization's privacy policies and practices must be understandable and easily available.
- **Individual Access:** Generally speaking, citizens have a right to access the personal information that an organization holds about you.
- **Recourse (Challenging compliance):** Organizations must develop simple and easily accessible complaint procedures. When you contact an organization about a privacy concern, citizens should be informed about avenues of recourse.

Appendix E: California Consumer Privacy Act

On January. 1, 2020, the California Consumer Privacy Act ("CCPA") came into effect. The CCPA applies to any for-profit entity that (i) does business in California, (ii) collects personal information of California residents (or has such information collected on its behalf), (iii) determines on its own or jointly with others the purpose and means of processing that information, and (iv) meets one or more of the following criteria: has annual gross revenues in excess of $25 million, adjusted for inflation; annually buys, receives for a commercial purpose, sells or shares the personal information of 50,000 or more consumers, households or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

CCPA has introduced the following non-exhaustive rights and obligations:

- Consumers have the ability to request a record of what types of data an organization holds about them, including what an organization is doing with a consumer's data regarding business use and third-party sharing.
- Businesses will have a process in place to verify a consumer is who they say they are when they make a request under CCPA.
- Consumers have a right to erasure subject to exceptions.
- Organizations will have to disclose to whom they sell data, and consumers will have the ability to object to the sale of their data.
- Sale of children's data will require express opt in, either by the child, if between ages 13 and 16, or by the parent if the child is younger than 13.
- Organizations cannot "discriminate against a consumer" who chooses to exercise their rights under CCPA.

UCTBRANDCUSTOMEREMPLOYEEPRODUCTBRANDCUSTOMEREMPLOYEEPRODUCTBRANDCUSTOMER

Qualtrics offers the world’s leading Customer Experience Management Platform. More than 10,500 enterprises worldwide, including half of the Fortune 100 and all of the top 100 business schools, rely on Qualtrics.

333 W River Park Drive Provo,
UT 84604

qualtrics.com