qualtrics XM

Cloud Security and Privacy Framework - Lite

Information, Security, Privacy, and Compliance

September 2021

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, refer 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: Research Core, Vocalize, Customer Experience, Employee Experience, Product 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.

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 hosted within the region where the Customer's primary data center resides, Data may be transferred and processed outside the data center region to comply with Customer requests or instructed (e.g., support purposes, use of sub-processor 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

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.

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.

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 at www.qualtrics.com/status.

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.

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.”

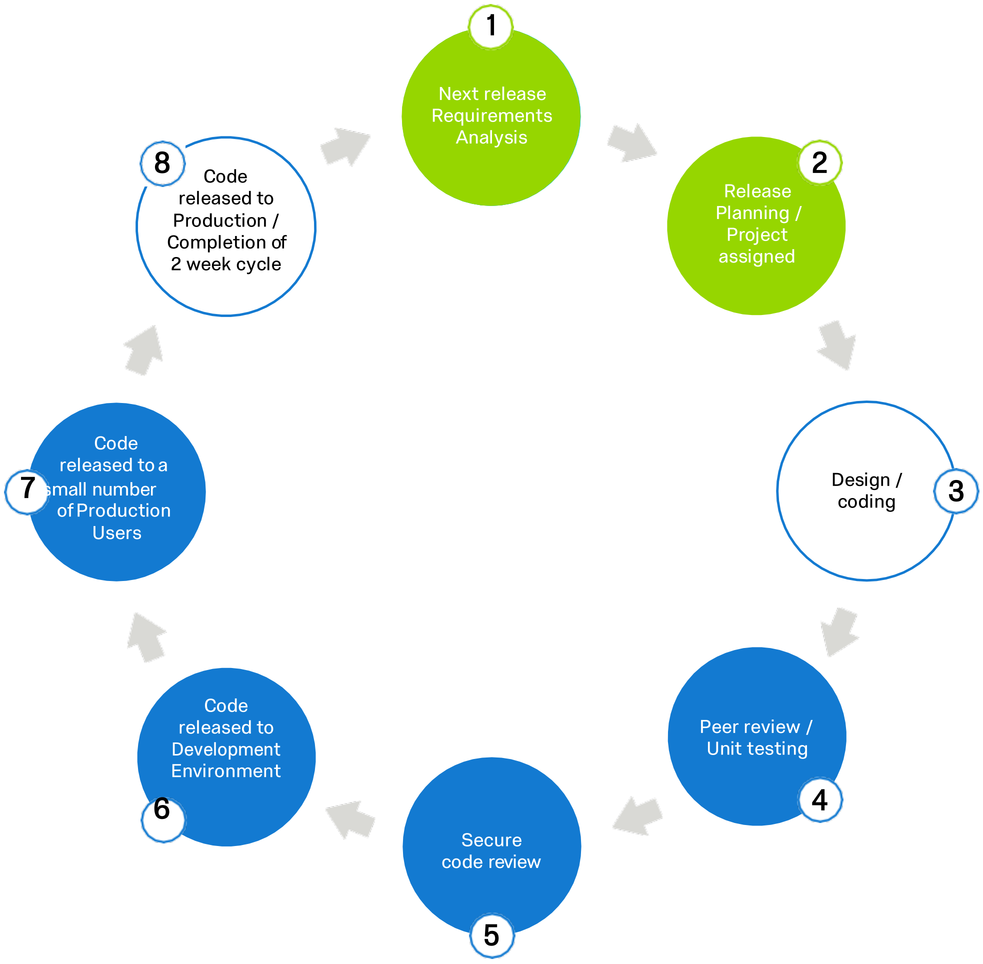
1
Next release Requirements Analysis
2
Release Planning / Project assigned
3
Design / coding
4
Peer review / Unit testing
5
Secure code review
6
Code released to Development Environment
7
Code released to a small number of Production Users
8
Code released to Production / Completion of 2 week cycle
●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

Figure 1. Development Methodology

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.

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 only processes Data to provide the Services.

Qualtrics treats all Data as highly confidential, and promises to safeguard Data as it would its own.

COMPLIANCE ASSIST

Qualtrics offers Compliance Assist as a tool 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.

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 enforces Transport Layer Security (TLS) v1.2 for all interaction with the platform and inside the platform through our service to service encryption. 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.

DATA ISOLATION ENCRYPTION (PREMIUM FEATURE)

As a premium security feature, Qualtrics offers Data Isolation. Data Isolation is an extra layer of encryption (AES 256-bit cipher) at the application layer with a unique customer key. This enables customer specific encryption and decryption of sensitive customer data in a multi-tenant system. Customer specific encryption keys (either Qualtrics managed or customer managed keys) are stored on Amazon Web Services' (AWS) Key Management Service (KMS).

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. BYOK allows a client to effectively destroy or deny access to their data in Qualtrics' possession. Clients provide us access to an AWS KMS master key to create and use data keys. Qualtrics' uses the client controlled and owned master key for data encryption and decryption. If a client declines Qualtrics access to their master key, Qualtrics can no longer decrypt or decipher that client's data. For additional information, see the Data Isolation Data Sheet.

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.

FULL DISK ENCRYPTION

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

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 are 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.

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.

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.

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

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

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.

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.

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.

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 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 security certifications:

SOC2 Type II Security, Confidentiality, Availability	**HITRUST** CSF v9.3	**FedRAMP** Government Data Standards (Moderate)
ISO 27001 Security Management Controls	**ISO 27017** Information Technology Security Techniques	**ISO 27018** Information Technology Security Techniques
IRAP PROTECTED- Level Controls	**CYBER ESSENTIALS** Cyber Threat Protection	

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.

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
- have access controls for 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
- are geographically diverse

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

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.

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.

Training and awareness

GENERAL SECURITY 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 computer security section of the employee manual includes the following topics:

- Privacy law compliance Physical
- security
- Email acceptable use policy
- Access control
- Internet security
- Personal devices in the company
- Information Security Incidents Password
- policy and tips
- Insider threat

Vulnerability management

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.

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).

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.

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.

Privacy Appendix

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 meaning and 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.

UCTBRANDCUSTOMEREMPLOYEEPRODUCTBRANDCUSTOMEREMPLOYEEPRODUCTBRANDCUSTOMER

qualtrics® XM

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