County of San Mateo ~ Special Services Review Form

Use this form for required special reviews (for contracts of any dollar amount) when the contract involves technology related services, construction services or leasing/property services as directed by Administrative Memo B-1 under Section I: General Provisions for all Contracts with Independent Contractors, paragraph J: Overview of Approving Authorities.

GENERAL INFORMATION

Contractor Name: Qualtrics
Contract Requestor Name: Juvy Ann Reyes

TYPE OF REVIEW

☒ **Information Services** ☐ **Public Works** ☐ **Real Property Services**

Comments from Contracting Department to Reviewing Department:
Please review the agreement between Qualtrics LLC and San Mateo County Health, PHPP for continuation and authorization to access the Cloud version of the Automated Contact Tracing and COVID-19 Patient Communication requirements. This was originally required in March 2020 as part of the State of Emergency related to COVID-19 throughout the State of California.

DEPARTMENTS: SUBMIT FORM FOR REVIEW TO:

For technology related contracts – e-mail this form to the Information Services Department: ***ISD-B1ContractReview@smcgov.org***
For construction or County owned facilities related contracts – e-mail this form to the Department of Public Works: ***pwcontracts@smcgov.org***
For contracts related to leased facilities – e-mail this form to Christine Hollender in Real Property Services: ***chollender@smcgov.org***

REVIEWING DEPARTMENT SELECT ONE OF THE FOLLOWING:

☐ **Special Review Completed**

☒ **Special Review Completed with Changes**

☐ **Special Review Completed but Not Recommended**

Comments from Reviewing Department to Contracting Department:
PHPP to work with CCO to add verbiage referencing vendor's Cloud Security and Privacy Framework – Lite document to section 7 of the contract to include "All Data is stored and processed in a single multi-tenant data center and in a single region(e.g. EU, US, Canada, Australia) chosen by the Customer. No Data is transferred outside of that region unless requested or instructed by the Customer (e.g., support purposes, use of subprocessor services) or as otherwise required for use of the Service."

REVIEWING DEPARTMENT AUTHORIZATION

Name of Department Reviewer: Mina Lim

Job Title of Department Reviewer: IT Analyst, Security Division, ISD

Date of Review: 12/9/2021

County of San Mateo – County Counsel Review Form

*County Counsel must review and approve **all** contracts over $100,000 and all contracts where changes are made to the standard contract templates before a contract is executed (for any amount). Review may also be requested for standard agreements under $100,000. Departments should work with assigned County Counsel to develop their own processes for review and approval. Where review is required, the Department must document approval by County Counsel in some format. In such situations, the Department may use this form, may develop its own review form, or may attach an email or other correspondence to show County Counsel approval.*

DATE: 12/10/2021

TO: Kate Broderick

FROM: Juvy Ann Reyes

SUBJECT: Agreement Review and Approval

Contractor Name: Qualtrics LLC

Maximum Contract Amount: $298,700

Rate of Payment: Monthly

☐ No changes to standard agreement form

☐ The following sections have been changed on the "standard" agreement:

Section No. and Title	Approved As Is *(For County Counsel Use Only)*	Modifications Required *(For County Counsel Use Only)*

Modifications *(Specify modifications to be made below; use additional paper if needed)*:

Not County Contract Agreement, we are using Qualtrics template.

☒ Approve agreement/exhibits/attachments

☐ Approve agreement/exhibits/attachments with modifications described above

Signature: Kate Broderick

Date: 12/16/2021

County of San Mateo ISD

Information Services Department
Technology Security Assessment

This document is to be completed for new or upgraded technology acquisitions, contracts, and projects. Please submit with all other proposals and agreement terms for review by the County Information Security Officer according to directives in Administrative Memorandum B-1. ***All questions must be answered fully.***

Submitting Department San Mateo County Health / PHPP / Epidemiologist **Submitter's Name** Edwina Williams / Karen Pfister

Phone 415

Section 1: Vendor Information

Name: Qualtrics, LLC | Corporate Phone #: 1-385-203-4999

Address: 333 W. River Park Dr. | City: Provo | State: UT | ZIP: 84604

Technical Support Contact Methods: *(Select all that apply)*
- ☑ Phone: 1-800-340-9194
- ☑ Email: benjamind@qualtrics.com
- ☑ IM/Chat
- ☑ Web Portal: https://www.qualtrics.com/support/

Technical Support Coverage Hours: ○ 24x7x365 ○ Business Hours M-F 8-5 Pacific ◉ Other: 5 Technical Account Manager hrs/week + 24/7/365 general support.

Does the vendor provide a dedicated account manager or representative for escalating problems or incidents? If yes, please provide name. ◉ Yes ○ No

If yes, please enter contact info here.
Ryan DePrima - rdeprima@qualtrics.com ; Elise Vu - elisev@qualtrics.com; Ben Danzger - benjamind@qualtrics.com

Does the vendor maintain any formal security policies & procedures to comply with industry requirements? ◉ Yes ○ No

How often is the vendor's security posture reviewed? See attached.

Will the vendor provide a copy of their last security audit? ◉ Yes ○ No

Does the vendor have any third-party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, TRUSTe or SOC 1/SOC 2/ SSAE 16/ISAE 3402? If yes, provide certification or attestations. ◉ Yes ○ No

Platform: ISO 27001/17/18, FedRAMP, HITRUST (HIPAA), SOC2 Type 2, Cyber Essentials

Data Centers: SSAE18/SOC2 Type 2, ISO27001

Section 2: Product Information

Product Name: Qualtrics Public Health Solutions | No. of Users: 1-10 | Does the product have technical constraints to the number of concurrent users it can support? ◉ Yes ○ No

☑ *This is an upgrade or renewal for existing technology currently in use in the County*

Location: ☐ *On-Premise* ☒ *Hosted (Cloud/Off-site)* ☐ *Hybrid (On-Premise/Cloud)*

Product Description and Purpose: ***Please include information that will identify the function, business process, and the departments/divisions who will use it.***

Solution is set at 105,000 responses. Additional charges will be applied if usage surpasses this response.

The following are high-level solutions:
Actions & Third Party Integrations - ability to maintain existing integrations with labs and third party vendors and stand-up patient portals to access data. SMC current has Health Connect Integration (Eurofins-Viracor, San Mateo County Public Health, Avellino) and Patient Portal Dashboards Business Portal solutions
Disease & Health Surveillance solutions - ability to develop health surveillance programs (Oral Health Surveillance, Rapid Health Assessments, and more)
Core Survey / Research Platform - ability to perform advance research and survey projects to collect information and analyze data
5 hours of Advance Technical Support to provide programmatic technical support, training and use-case development

Integration: Does the product integrate or interface with any other existing or planned products or services used either at the County, or with another third-party County vendor? This would include requirements for integration or use of the County's email System, ServiceNow, or other systems. ◉ Yes ○ No

SFDC: Contact tracers make referral requests within CalConnect and a Qualtrics-Salesforce integration is utilized to send these requests to a survey in Qualtrics to kick off the individual swab process.

HL7: Health Connect integrations with labs (Eurofins-Viracor, SMC Public Health Lab, Avellino) to send COVID-19 test results into Qualtrics and disclose results for Public Health Lab administered tests.

Has the application been subjected to any breaches? If yes, include separately, enacted steps to mitigate including response and escalation processes. ○ Yes ◉ No

Not that we are are aware of. Any suspicious activity is logged and investigated. The numbers and types are kept confidential.

Known Vulnerabilities? ○ Yes ◉ No

See attached.

Data Sensitivity: ☐ Public ☐ Internal ☐ Confidential ☐ Restricted

Data Criticality: ☐ **Useful** ☐ **Important** ☐ **Essential** ***For details on Data Sensitivity and Data Criticality, please see the References section of this document***

Section 3: Administrative Controls

Configuration and System Hardening: Does the product offer a baseline configuration or system hardening tool that can protect the product against confidential data disclosure or service disruption? **Please provide system configuration diagram

○ Yes ◉ No — See attached.

Backup and Restore: Does the product offer features to backup and restore user data, configurations, and application code?

◉ Yes ○ No — See attached.

Does the product integrate with Rubrik Storage Services and API (the County's backup platform)?

○ Yes ○ No

If there is a backup process performed by Vendor: ◉ Yes ○ No

How often: Daily

Encrypted? ◉ Yes ○ No

Retention period: 90 days

Where stored? Amazon

Data at Termination of Agreement: Will the data be returned?

○ Yes ◉ No

What assurance is provided for complete removal?

See attached.

Section 4: Security Controls

Monitoring and Event Management: Describe how the product can be monitored for performance, reliability, and security. Include how the product reacts to events that are raised during normal operations.

See attached.

Can the product forward events to a central log repository or System Event and Incident Management (SEIM) platform

◉ Yes ○ No

Patching: Describe how the product is patched and updated. Include how frequently the vendor provides security fixes and updates.

See attached.

If the hardware is onsite, can County engineers apply patches

○ Yes ○ No

If hosted, please provide version, service pack, patches, and how will the server be maintained to the lasted patch level?

See answer above.

Malware Protection: Will the product be affected by servers or endpoints that run anti-virus/anti-malware protection? If yes, provide details on what exclusions are required for the product to work effectively.

◉ Yes ○ No — See attached.

Employees: Have employees undergone a background check process?

◉ Yes ○ No

Will the provider use a subcontractor or 3rd party service provider?

◉ Yes ○ No

If yes, please attach and provide for each subcontractor, the security and privacy agreement.

See attached.

SaaS: Is the product 100% web-based?

◉ Yes ○ No

What are the browser security configuration requirements?

See attached.

Is the portal ADA compliant with Section 508 of the Rehabilitation Act and follows the principles of responsive web design?

◉ Yes ○ No

Disaster Recovery: Is the location of the server, if hosted, in an area prone to natural disaster?

◉ Yes ○ No — San Jose, CA

Is there a disaster recovery plan in place?

◉ Yes ○ No

What is the guaranteed uptime? See attached.

RTO: 24 hours RPO: < 4 hours

Identity and Authentication Management:
Does the product provide for, or support *identity and authentication integration with via other credentialing systems or protocols?*
Note: SAML 2.0 and OAuth 2.0 are the preferred choice for integration with San Mateo County systems (older versions are not compatible).

****If OKTA integration is selected for application integration, answering the Password Management section below will not be required.***

(●) Yes ( ) No If yes, please specify

[✔] SAML [✔] Active Directory
[ ] OAuth [✔] LDAP
[ ] MFA [✔] Other Google OAuth 2.0, CAS

Password Management:

How are accounts provisioned and managed (include deprovisioning and removal)?

See attached.

Does the product provide for password management that meets the County password policy for complexity, expiration, reuse, and lockout? ***See References section for more information about San Mateo County's Password Policy***

(●) Yes ( ) No

1. All users have a single account with unique account ID? (●) Yes ( ) No
2. First time password must be unique and changed upon initial login? (●) Yes ( ) No
3. Password must be changed every 60 days? (●) Yes ( ) No
4. Password must have at least 8 characters and 1 character from 3 of: lowercase, uppercase, number, and special character? (●) Yes ( ) No

Does the product provide for password self-reset capability? (●) Yes ( ) No

How are passwords stored? Encrypted? (●) Yes ( ) No

Access Management: Does the product allow for privileges to be assigned to both individuals and 'groups' of individuals in order to support the use of 'Roles' for access permissions? Please describe method used. (●) Yes ( ) No

See attached.

Encryption: Identify and describe whether the product encrypts data during different states – i.e., at rest, in use, and in transit. Also include credentials (usernames, passwords, etc).

Data-in-transit	See attached.
Data-in-use	
Data-at-rest	All data is encrypted in transit and at rest.
Credentials	See attached.

Auditing: Does the product provide a mechanism for auditing system activity and/or reporting of that activity? Examples of auditing include user login/logoff, user actions, data export, and permission changes. (●) Yes ( ) No

See attached.

Section 5: Cloud/Hosted Services

Data Sovereignty: Does the vendor keep all the data within the United States? Please provide location(s) where San Mateo County's data will be stored.

See attached.

Tenancy: Describe how San Mateo County data resides with other customer data in the hosted environment-- i.e., is the data co-mingled in a single database, or are there separate customer databases?

See attached.

Hosted Platform: Please describe the vendor's technology platform in the hosted environment-- both application, database, and/or other layers (e.g., Ruby on Rails, Redis Cache, MongoDB)

Details are not released.

Third Party Services: Does the vendor use any third-party services (e.g., for development, QA, helpdesk, integration services, offsite backup locations, etc.) where the third party vendors have access to San Mateo County data? (●) Yes ( ) No

See www.qualtrics.com/subprocessor-list for the list of subprocesses and services provided.

Network Defenses: Please describe how the vendor's network perimeter is protected, including whether an IPS/IDS and anti-virus system is activated, and whether there is a central logging facility for perimeter events

See attached.

Service Levels and Incident Response:
What is the service level for this hosted product, and how does the vendor guarantee that level for its customers? Include how the vendor notifies customers of incidents that do not meet service levels.

This is defined within the MSA.

Data Loss Events: Has the vendor experienced any data loss incidents which required reporting to regulatory authorities in the past 24 months?
( ) Yes (●) No

If yes, please provide additional details.

Forensic Analysis: Who would perform a forensic analysis of a breach if one were to occur at the vendor site?	Qualtrics
IP Restrictions: Does the vendor's hosted site have the capability to restrict access to San Mateo County's public IP address space? (●) Yes ( ) No	Yes, Qualtrics has the ability to restrict access to the client's instance to specific IP addresses.

Section 6: References

Password Policy

The County of San Mateo's Information Security Policy requires new technology implementations that use passwords to adhere to the following password requirements:

County of San Mateo Password Requirements

1. All users must have unique account IDs that identifies a single account owner
2. First time password must be unique to an individual, and require change upon initial login
3. The permanent / long term password requires an enforceable change every 60 days
4. The password must enforce a minimum of at least 8 characters, and contain at least one character from three of the following:
    a. Lower Case
    b. Upper Case
    c. Numbers
    d. Special Characters

Data Classification Standards

In order to apply the proper security safeguards to digital assets, the County of San Mateo classifies new technology both to a Sensitivity and Criticality class. The following information defines those classification standards, and is added as a resource to answering the questions in Section 3, 'Product Information'.

Sensitivity Class	Description
Public	Public data is information assets that can be disclosed without restrictions. Permission to release or share data does not require approval. Examples: • Information typically included on the San Mateo County website— County addresses, department phone numbers, generic department emails, • Applications, request forms, press releases
Internal	Internal data is intended to be used only within San Mateo County, but disclosure poses minimal business impact, and may even be subject to release per the County's Open Data Policy. Permission to share publically is to be given by the data steward or through committee approval. Examples: • Business plans, budgets, vendor lists, vendor contracts • Memo's, meeting minutes, policies/procedures
Confidential	Confidential data is information assets that, if compromised, could adversely impact customers or San Mateo County business. This information is to receive data protection for storage and transport, should only be used for business purposes, and where possible be identified as confidential by those who use it. Examples: • Social Security Numbers, Driver's license number, credit cards • Personal addresses, phone numbers, private email addresses • Access codes or passwords A compromise of Confidential data is to be reported as a security incident, as outlined in the County's Incident Response Plan.
Restricted	Restricted data is Confidential data—except, the business impact for compromise is much greater. This includes civil penalties, regulatory redaction for organizational credentials, and formal notification to federal, state, and local authorities. Restricted data typically involves information that has contractual, legal, or regulatory obligations to protect the data in the utmost manner. Examples: • Medical Records and other Protected Health Information (PHI) • Employee criminal background checks The organization as a whole– along with data stewards– is responsible for designating data as Restricted. A compromise of Restricted data is to be reported as a security incident, as outlined in the County's Incident Response Plan, and included notification to the County's Privacy Officer.

Criticality Class	Description
Useful	Useful data is information assets helpful to the mission of the health system, but whose availability isn't necessary to maintain day-day operations. Useful data is often characterized with low risk in case of loss or compromise. Examples: • Printers and Fax machines where there are multiple alternatives • Images of workstations that can be rebuilt if necessary • Training materials • Reports that can be reproduced from original sources
Important	Important data is information assets whose availability is valuable for maintaining day-day operations, but service-levels can tolerate an unscheduled period of downtime. Downtime for Important data is acceptable at certain days/hours in given week, but usually no longer than three (3) consecutive days for any single event. Examples: • Software systems that are only used during the weekday and/or normal business hours • Software systems where data sets updates are not updated frequently, and business tasks can be deferred without service impact • Managed Services run by the State of California • Systems where contingency plans can maintain service levels
Essential	Essential data requires nearly continuous uptime. Business processes are adversely affected with even a small amount of unscheduled downtime, impacting the job performance of the workforce and services to customers. Access to these information assets typically requires 24x7x7 availability, and must be rigorously protected. Examples: • EMR Systems • Identity Management Applications • Core networking equipment

Section 7: Non-Compliance

Please explain area(s) of non-compliance. Provide information as to the services or systems that would be impacted as well as the proposed remediation, if any.

NOTE: All Non-Compliance must file an Information Security Risk Acceptance Form

Please explain areas of non-compliance.

Section 8: Other Documents

Please include any pertinent documents, diagrams of network, and/or data flow architecture

Documents included? (•) Yes ( ) No

This assessment was prepared by (Print Name) Trevor McDougal

Signature Trevor McDougal

Date 18-October-2021

Phone _____

How often is the vendor's security posture reviewed?

Information security policies and procedures are reviewed and updated at least annually.

Known Vulnerabilities?

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.

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 production 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.

Qualtrics does not allow customers to perform their own scans, nor do we release tests. Please refer to our Qualtrics Cloud Security and Privacy Framework for confirmation of our high security standards.

Configuration and System Hardening: Does the product offer a baseline configuration or system hardening tool that can protect the product against confidential data disclosure or service disruption? **Please provide system configuration diagram.

Qualtrics is a self-service tool and the use of it is determined by the customer. However, their are control recommendations documented within the SOC2 Report and Cloud Security and Privacy Framework document.

Backup and Restore: Does the product offer features to backup and restore user data, configurations, and application code?

Qualtrics has disaster recovery and business continuity plans in place. All services have quick failover points with redundant hardware, and encrypted backups are performed nightly, including automatic propagation across servers (immediate upon collection).

Since customers own and control their data, they are responsible for accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of the data. They are also responsible for data backup (there are numerous download formats and mechanisms) and retaining the backup according to their retention policy. Depending on how live data were deleted, it may be possible for the user to undelete it using a feature of the Qualtrics platform. If that feature is unavailable, then the user must restore from a personal backup. Survey definitions, response data, and some other data may be easily exported to the user's own system for backup. This is highly recommended as Qualtrics is under no obligation to restore data not caused by its own negligence.

Daily backups of the entire Qualtrics services are retained for 90 days. However, restoration of this data is only for disaster recovery. The backups are electronic (no tape) and stored in an alternate data center in the region it was created (US/EU/Asia-Pac).

What assurance is provided for complete removal?

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. You own your data and have 100% access to it at all times throughout your contract, allowing you to download or remove it at any time.

Monitoring and Event Management: Describe how the product can be monitored for performance, reliability, and security. Include how the product reacts to events that are raised during normal operations.

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 event s 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.

Patching: Describe how the product is patched and updated. Include how frequently the vendor provides security fixes and updates.

The Qualtrics Engineering Team is responsible for managing all activities regarding information system flaws. Information system flaws are identified, reported, and corrected via the following procedures: flaws are first discovered via the Department of Homeland Security (DHS), US-CERT advisories, news articles, or vulnerability scans. Scans of the operating system and databases are conducted on a quarterly basis to initially identify system flaws. The results of these scans are then analyzed to determine if the associated findings are legitimate or false positive. All legitimate findings are then tracked through the JIRA ticketing system. When US-CERT notifications are received, they are evaluated and appropriate actions are taken on the Qualtrics infrastructure to mitigate vulnerabilities and protect against threats. The Engineering Team considers each threat and its potential impact on the organization when setting priorities for remediation. Factors that are considered during the evaluation are the significance of the threat or vulnerability; the existence, extent, and spread of related worms, viruses, or exploits; and the risks involved with applying the patch or non-patch remediation. Any system flaws that are identified as part of this process added to a plan of action and milestones (POA&M) for tracking and remediation. If the advisory is identified as not affecting the Qualtrics environment, the JIRA ticket is closed. If the flaw requires a change in the configuration, the change must be approved through the change request process (configuration/change management). All patches are updated in production systems during the maintenance window unless it is an emergency patch that requires a faster response. Emergency patches that require systems to be taken offline temporarily

and that are outside the normal patch window will be communicated to the affected end-user/customers via email. The email will inform the users/customers of the system(s) that will be affected and the estimated downtime. Updates and patches are tested by the Engineering Team prior to implementation in the staging environment

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 that 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.

Malware Protection: Will the product be affected by servers or endpoints that run anti-virus/anti-malware protection? If yes, provide details on what exclusions are required for the product to work effectively.

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.

If yes, please attach and provide for each subcontractor, the security and privacy agreement.

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.

Checks are administered by Sterling Talent Solutions and, in where allowed by applicable law, candidates are screened for identity verification, education verification, employment verification, and criminal checks (where allowed by law), and more (i.e. in the U.S. this includes SSN trace, extended global sanctions, DOJ sex offender, and locator select and verification). Qualtrics individually assesses each background check. Qualtrics considers job duties and time passage, among other factors, in determining what constitutes satisfactory completion of the background check.

All information obtained as a result of a background check will be used solely for employment purposes. Certain customers require updated and/or additional background checks for Qualtrics employees. Qualtrics reserves the right, with employee's consent, to conduct additional background checks for employees working on specific customer accounts. All background check information will be held confidential. Qualtrics complies with all applicable local, state, federal and international laws regarding background checks. Falsification or omission of information related to a background check may result in denial of employment or discipline, up to and including termination.

What are the browser security configuration requirements?

Qualtrics is a fully hosted online solution, and there are no set hardware or operating system requirements. Only a modern web browser with internet access is required. All major web browsers are supported (Apple Safari, Google Chrome, Microsoft Edge/Internet Explorer, Mozilla Firefox). No installation is required.

What is the guaranteed uptime?

99.97% average up-time since 2010.

How are accounts provisioned and managed (include deprovisioning and removal)?

Accounts can be created manually by a Brand Administrator, or created by users with Self-Enrollment enabled. Admins can use self-enrollment codes that users can enter to create an account with specific permissions tied to each code. With SSO enabled, user accounts can be created automatically when users successfully authenticate and don't yet have an account on your brand. Users can be managed by any brand admin; changes can be made on a user-by-user basis, and coupon codes can be generated for larger groups of users to enter in the platform and change their user permissions. Admins can disable or delete accounts manually, or set an expiration date for an account ahead of time.

Access Management: Does the product allow for privileges to be assigned to both individuals and 'groups' of individuals in order to support the use of 'Roles' for access permissions? Please describe method used.

Admins can create user types, which are templated permission configurations that can be assigned to new and existing users. In order to assign the same user type to a large

group of users, admins can utilize coupon codes that users enter in their accounts to change their account permissions.

Encryption: Identify and describe whether the product encrypts data during different states–i.e., at rest, in use, and in transit. Also include credentials (usernames, passwords, etc).

Data-in-transit

Qualtrics uses Transport Layer Security (TLS) encryption for all transmitted Internet data (HTTPS [TLSv1.2 with AES 128/256]).

Credentials

Passwords are never accessible to Qualtrics. Qualtrics does manage the encryption keys for all customers not using our Data Isolation premium feature with Bring Your Own Key. Only customers who pay for this additional feature have keys not controlled by Qualtrics.

Auditing: Does the product provide a mechanism for auditing system activity and/or reporting of that activity? Examples of auditing include user login/logoff, user actions, data export, and permission changes.

Admins have access to reports on user activity (and ability to export this data) -- number of new users over time, platform usage, total logins and unique users over time, account creation date and last login date. Admins also have the ability to proxy login to other users accounts and set a time after which inactive accounts will be disabled automatically. Permission changes are not tracked.

Data Sovereignty: Does the vendor keep all the data within the United States? Please provide location(s) where San Mateo County's data will be stored.

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.

US East— A hosting facility located near Washington, D.C.
US West— A hosting facility located in San Jose, CA

Tenancy: Describe how San Mateo County data resides with other customer data in the hosted environment-- i.e., is the data co-mingled in a single database, or are there separate customer databases?

Qualtrics' multi-tenant solution includes a shared Database and Schema (all client data is stored in a shared database and schema and data is separated by SQL query filters). Qualtrics logically segments all customers and data on the platform. This is done by organization, username/password combination, as well as survey ID unique to each survey.

Network Defenses: Please describe how the vendor's network perimeter is protected, including whether an IPS/IDS and anti-virus system is activated, and whether there is a central logging facility for perimeter events

Each data center, as well as the Qualtrics HQ, has high-end firewall systems with IDS/IPS capabilities enabled. Each packet is analyzed for malware and other properties and, if validated, quarantined to physically separated and segmented back-end systems.

Guidelines for IT Contract Review

San Mateo County requires a Special Services review for contracts that include Information Technology (IT) goods and services. The Health IT Division (HIT) has created the IT Contract Review Checklist which should be completed for any proposed contract that includes IT goods and services. The Health IT Division will collaborate with the requesting Division on achieving concurrence on Special Services reviews with ISD using the following workflow:

1. While negotiating with a potential vendor, please ensure you complete the IT Contract Review Checklist attached below.
2. Save your document using the following naming convention: SSR-your division-vendor's name. For example, the file name of the document could read "SSR-SMMC-Picis.docx." Send the completed IT Contract Review Checklist along with the completed County B1 Review form (Special Services Review Form), Technical Security Assessment Questionnaire (completed by vendor), Vendor Agreement and additional required documents related to this contract to:

   HS_HIT_Contract_Review@smcgov.org

3. HIT will review completed submissions within five business days of receipt of a complete package. If there are no follow-up questions, HIT will forward your documents to ISD for concurrence on the County B1 Review form. The ISD review can take up to ten business days.
4. The HIT Contract Administrator will keep you apprised of the status of the review by email.
5. The HIT Contract Administrator will return the signed Special Services Form to your Division. You may then proceed with the completion of your Division's contract approval process.
6. Should you have questions, please contact Cyndy Chin at cchin@smcgov.org.

FAQ'S

1. What is required for the Scope of Work?
   a. Description of Service
   b. Agreement Terms
   c. Amount and method of payment
   d. Service Level Agreement (SLA)
   e. Purpose
   f. Location of Work
   g. Period of Performance
   h. Deliverables
   i. Application Standards
   j. Acceptance Criteria
   k. Special Requirements, if any

2. What is required in a Service Level Agreement (SLA)?
   a. Availability
   b. Performance
   c. Capacity
   d. Disaster Recovery

3. What is required for an Implementation plan?
   a. Project Plan for installation
   b. Resources outlined (Health IT, Health SMMC, ISD, Vendor)
4. What is required for a Support plan?
   a. List of covered / support devices and/or processes
   b. Coverage level agreements (24/7, 5/8)
   c. High-level process for trouble tickets
   d. Contact information (phone#'s, email)

IT Contract Review Checklist

Department: San Mateo Count Health / PHPI Contact: Karen Pfister and Edwina
Vendor Name: Qualtrics
Type of Review: Agreement

What is the Purpose of this Contract and General Information

What was the situation before identifying requirement of this service, how was it determined that the County requires this service, how was this contractor selected, *(no more than 1200 characters).*

Data Personal Data (Cloud Service). This DPA applies to Personal Data processed by Qualtrics and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by Qualtrics, and Customer shall not store Personal Data in such environments. The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Technical Account Manager (TAM)
The TAM will focus primarily on high value-add activities for Customer, including strategic technology thought partnership, formal program technology reviews, optimizing technology decisions, escalation management, training, and revision activities. The TAM will work in conjunction with other specialists to help diagnose, troubleshoot, and resolve technical support queries from the Customer.

NTE Amount: $248,700.00 **TERM: from** 06/30/2021 **to** 06/29/2022

Have You Received?

- **Vendor's Certificate of Insurance?** (●) **YES** ( ) **NO**

If not on County Template:

- **Is Disentanglement included in Agreement?** ( ) **YES** (●) **NO**
- **Is Warranty for product or service included in Agreement?** ( ) **YES** (●) **NO**

Required Documents: (Please attach to this form)

- County Agreement that includes Scope of Work (SOW) and contract pricing.
- Supporting Vendor Documents which are to include:
  - Service Level Agreement (SLA) and Support Plan
  - System/Service Overall and Technical Specifications
  - Implementation Plan
- **Completed Review Form:** Technology Security Assessment Questionnaire
- **Completed Review Form:** ISD Special Services Review Document

County of San Mateo
Health Insurance Portability and Accountability Act (HIPAA) Questionnaire

Date: 11/22/2021

Contractor Name: Qualtrics LLC

Contract Administrator: Juvy Ann Reyes

Answer the following questions to determine if the Contractor is Business Associate

1. Will the County disclose individually identifiable health information concerning County clients to the contractor?

   ☒ YES (if this box is checked, go directly to question #3)

   ☐ NO (if this box is checked, respond to question #2)

2. Will the Contractor use individually identifiable health information concerning County clients in the process of providing services for the County?

   ☒ YES

   ☐ NO

   If you responded "NO" to **both** questions #1 and #2 then **stop here**. This is **not** a Business Associate. If you answered "YES" to either #1 or #2, then proceed to question #3

3. Will the Contractor use the identifiable health information ***ONLY*** to provide direct physical/mental health care or treatment to clients of the County?

   ☐ YES (if this box is checked, this **is not** a business associate)

   ☒ NO (if this box is checked, the contractor **IS** a business associate)

4. Explain the services provided by the Contractor:
   Contractor will implement the Automated Contact Tracing and COVID-19 Patient Communication project to ensure the County of San Mateo is effectively and efficiently communicating with COVID-19 Cases and corresponding Contacts.

Name of person completing/approving this form: Marc Meulman
Director of Public Health, Policy and Planning

Date:

Approved By:

Questions about HIPAA should be directed to the San Mateo County HIPAA Privacy Officer and/or County Counsel.

County of San Mateo ~ Insurance Certification Questionnaire

Contractor Name: Qualtrics LLC

Contract Number: TBD

Date this Form Was Completed: 11/17/2021

Name of Person Completing Form: Juvy Ann Reyes

1. Does the contractor carry $1,000,000 or more in comprehensive general liability insurance? *(For Health System only, does the professional (MD, psychologist, nurse) work in a hospital setting where the facility will cover the general liability?)*	☒ **YES**	☐ **NO***
2. Does the contractor travel by car to provide contract services?	☒ **YES**	☐ **NO**
a) If yes, does the contractor carry $1,000,000 or more in motor vehicle liability insurance?	☒ **YES**	☐ **NO***
3. Does the contractor have 2 or more employees?	☒ **YES**	☐ **NO**
a) If yes, does the contractor carry statutory limits (see handbook) for Workers' Compensation insurance?	☒ **YES**	☐ **NO***
4. Is this a contract for professional services (state certification, architect, accountant, physician, etc.)?	☐ **YES**	☒ **NO**
a) If yes, does the contractor carry professional liability insurance?	☐ **YES**	☐ **NO***
5. Did you make any changes to the Hold Harmless clause in the contract template?	☒ **YES**	☐ **NO**
a) If yes, did Risk Management and County Counsel approve changes to the contract template?	☒ **YES**	☐ **NO***
6. Is San Mateo County named as the certificate holder / additional insured?	☐ **YES**	☒ **NO***

If "No*" is checked in any of the red asterisk boxes (#1, #2a, #3a, #4a, #5a, or #6) – call Risk Management for further instructions...otherwise, this form is complete. Attach the completed form to the insurance certificate and keep both documents with the contract packet.

COMMENTS:

Section below is for Risk Management authorization – send to Risk Management **ONLY IF INSTRUCTED TO DO SO**

Risk Management has reviewed and approved modification or waiver of insurance requirements for this contract.

Risk Management Signature: Click here to enter text. **Date:** Click here to enter a date.

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
04/06/2021

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Services Central, Inc.
Philadelphia PA Office
One Liberty Place
1650 Market Street
Suite 1000
Philadelphia PA 19103 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122 **FAX (A/C. No.):** (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	National Union Fire Ins Co of Pittsburgh	19445
INSURER B:	AIU Insurance Company	19399
INSURER C:	New Hampshire Insurance Company	23841
INSURER D:	XL Insurance America Inc	24554
INSURER E:		
INSURER F:		

INSURED
SAP America Inc
Attn: Kathleen O'Donnell
3999 West Chester Pike
Newtown Square PA 19073 USA

COVERAGES **CERTIFICATE NUMBER:** 570086915764 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
D	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PRO-JECT LOC OTHER:			US00099181LI21A SIR applies per policy terms & conditions	04/01/2021	04/01/2022	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG Pers/Adv Inj SIR	$1,000,000 $100,000 $5,000 $1,000,000 $2,000,000 $3,000,000 $650,000
A	**AUTOMOBILE LIABILITY** X ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS NON-OWNED AUTOS ONLY			CA 1722408	09/30/2020	09/30/2021	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$2,000,000
D	X **UMBRELLA LIAB** X OCCUR **EXCESS LIAB** CLAIMS-MADE DED X RETENTION			US00099182LI21A SIR applies per policy terms & conditions	04/01/2021	04/01/2022	EACH OCCURRENCE AGGREGATE	$5,000,000 $5,000,000
B	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N: N **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		WC048425978 20-21 WC AOS	09/30/2020	09/30/2021	X PER STATUTE OTH-ER	
B				WC048425979 20-21 WC CA	09/30/2020	09/30/2021	E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT	$1,000,000 $1,000,000 $1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
See Addendum.

CERTIFICATE HOLDER

SAP America Inc.
Attn: Kathleen O'Donnell
3999 West Chester Pike
Newtown Square PA 19073 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services Central, Inc.

Holder Identifier :

Certificate No : 570086915764

AGENCY CUSTOMER ID: 10194755
LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services Central, Inc.	SAP America Inc
POLICY NUMBER: See Certificate Number: 570086915764	
CARRIER: See Certificate Number: 570086915764 / NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 **FORM TITLE:** Certificate of Liability Insurance

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER	
INSURER	
INSURER	
INSURER	

ADDITIONAL POLICIES If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS	
	WORKERS COMPENSATION							
B		N/A		WC048425980 20-21 WC FL	09/30/2020	09/30/2021		
C		N/A		WC048425981 20-21 WC - MA ND OH WA W	09/30/2020	09/30/2021		

AGENCY CUSTOMER ID: 10194755
LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services Central, Inc.	SAP America Inc
POLICY NUMBER	
See Certificate Number: 570086915764	
CARRIER / NAIC CODE	EFFECTIVE DATE:
See Certificate Number: 570086915764	

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 **FORM TITLE:** Certificate of Liability Insurance

Description

The Named Insured includes SAP America, Inc. and its subsidiaries and affiliates including, but is not limited to the following:

SAP America, Inc.
SAP Global Marketing Inc.
SAP National Security Services, Inc.
SAP Industries, Inc.
SAP International, Inc.
SAP Labs, LLC
SAP Public Services, Inc.
TomorrowNow, Inc.
iAnywhere Solutions, Inc.
Sybase 365, LLC
Sybase, Inc.
Ariba, Inc.
SmartOps, Inc.
KXEN, Inc.
SuccessFactors, Inc.
hybris (US) Corporation
Plateau Systems, Inc.
Fieldglass, Inc.
SeeWhy, Inc.
Concur Technologies, Inc.
TRX, Inc.
Altiscale, Inc.
Hipmunk, Inc.
Gigya, Inc.
Callidus Software, Inc.
Technology Management Associates, Inc.
Apex Expert Solutions, LLC
Qualtrics International, Inc.
Qualtrics LLC, Wilmington, DE, United States
Delighted LLC, Wilmington, Delaware, United States
Volume Integration, Inc., VA, United States
Emarsys NA

Commercial General Liability:

Additional Insured is included when required by written contract and in accordance with the policy provisions of the Commercial General Liability policy.

AGENCY CUSTOMER ID: 10194755

LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Aon Risk Services Central, Inc.	SAP America Inc
POLICY NUMBER	
See Certificate Number: 570086915764	
CARRIER / NAIC CODE	EFFECTIVE DATE:
See Certificate Number: 570086915764	

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: ACORD 25 **FORM TITLE:** Certificate of Liability Insurance

Description

Waiver of Subrogation is granted when required by written contract (except where not permitted by law), in accordance with the policy provisions of the Commercial General Liability.

Primary and non contributing status shall apply when required by written contract and in accordance with the policy provisions of the Commercial General Liability policy.

Automobile Liability:

Additional Insured is included when required by written contract and in accordance with the policy provisions of the Automobile Liability policy.

Waiver of Subrogation is granted when required by written contract (except where not permitted by law), in accordance with the policy provisions of the Automobile Liability policy.

Auto Liability Coverage is primary for any liability assumed when required by written contract.

Workers' Compensation:

Workers' Compensation Policy #WC048425981 includes employer's liability for monopolistic states of North Dakota, Washington, Wyoming, Ohio.

Waiver of Subrogation is granted when required by written contract (except where not permitted by law), in accordance with the policy provisions of the Workers' Compensation policy.

Umbrella/Excess Liability:

Please note that because the Umbrella/Excess policy terms follow the underlying policies, there are no separate additional insured, waiver of subrogation and primary and non-contributory endorsements applicable to this policy.

qualtrics XM

Qualtrics, LLC
333 W. River Park Dr.
Provo, UT 84604
support@qualtrics.com
(801) 374-6682

To whom this may concern,

This letter serves to notify you that Qualtrics, LLC is the sole provider of the leading research and insights platform available on www.qualtrics.com, offering the unique combination of technology and expertise as detailed below:

- Advanced website targeting: website feedback software to pinpoint web visitors with targeted messaging using over 20 behavioral, location, and device-type variables.
- Data Ownership: Customers own and control all data entered in or collected by Qualtrics technology. This includes survey definitions, questions, response data, panel data, and uploaded content such as graphics, user information, and report results/analysis from such data.
- Data analysis: Real-time reporting, flexible dashboards, text analytics, Bain Certified NPS and benchmarking, can all be gauged and generated within the insight platform.
- Collaboration: The platform allows surveys, messages, and libraries to be collaborated or shared only within the 1.2 million users of Qualtrics.
- Employee Insights: Qualtrics provides multi-rater assessments, employee engagement surveys, hierarchical reporting, and onboarding feedback and exit surveys.
- Integration: The platform supports integrations with external systems (CRM platforms, email service providers, analytics and reporting platforms, HRMS/HRIS systems, and more). Other integrations include Microsoft Dynamics, Salesforce, Adobe Sitecatalyst, Oracle CRM, SAS, Twitter, Facebook, SQL server, PeopleSoft, Google Analytics, PayPal, YouTube, Marketo, Tableau, among others.
- Security: All Qualtrics products enable customers to control individual permissions for their accounts, web intercepts, dashboards and surveys.
- Web Intercepts: These can be completely customized with images, text and logos and provides a built-in rich text editor and HTML view. Said web intercepts can only be integrated in and used with the Qualtrics survey platform.
- Libraries: The platform offers a unique global resource library of surveys, questions, and images that can be used for survey creation only within the Qualtrics platform.
- Duplication Management: The platform automates de-duplication within distribution lists for more targeted outreach.
- Subject matter expertise: In addition to market-leading technology, Qualtrics provides subject matter expertise to optimize each unique project with the best industry and research resources available.
- SMS: The platform supports surveys taken through Short Message Services (SMS).
- Administration: The platform allows administrators and sub-administrators to manage the various user accounts. The platform also has a built-in survey approval process that requires surveys to be previewed and approved before distribution. This is unique to Qualtrics technology.
- Vocalize: This dashboard product integrates with the Insights Platform to visualize data in real time, filter results for permission-based access, and allow for text analytics and closed-loop case management.

Best regards,

Mark Creer, Director
Qualtrics, LLC

qualtrics XM

Cloud Security and Privacy Framework - Lite

Information, Security, Privacy, and Compliance

November 2020

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, Australia) chosen by the Customer. No Data is transferred outside of that region unless requested or instructed by the Customer (e.g., support purposes, use of subprocessor services) or as otherwise required for use of the 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 does not disclose any Data to third parties. Qualtrics treats all Data as highly confidential, and promises to safeguard Data as it would its own.

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 cannot classify or represent the Data. All Data is treated as highly 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 atwww.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."

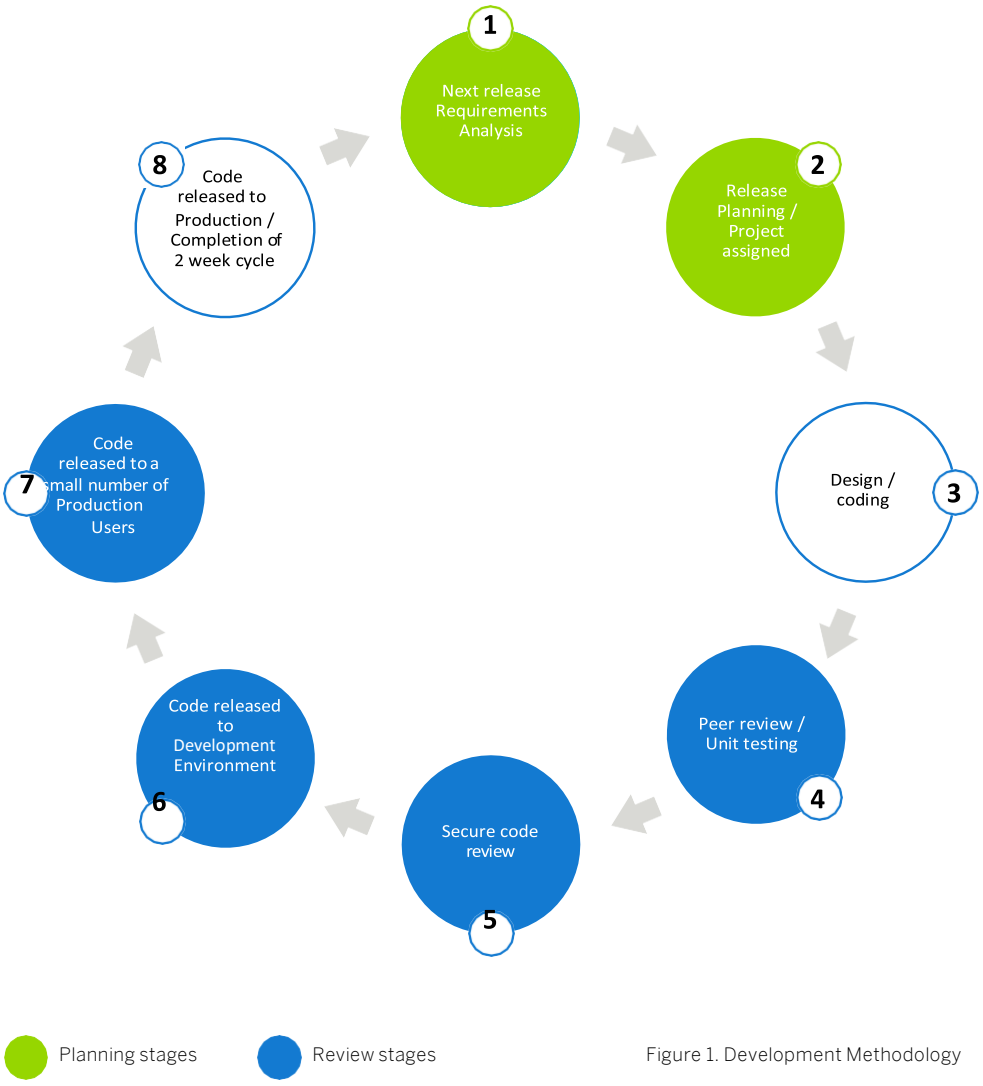

Figure 1. Development Methodology

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.

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 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 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.

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.

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

The 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

ISO 27001
Security Management Controls

FedRAMP
Government Data Standards (Moderate)

CYBER ESSENTIALS
Cyber Threat Protection

HITRUST
CSF v9.3

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
- 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.

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 newpassword.
- **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- factorauthentication(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:

- InsidethePlatform: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 meaningand protects Data using industry-standard security practices.

All EU Data collected in an EU data center are stored and processed there; Data are never transferred outside the EU by Qualtrics unless requested or instructed by Customer i.e. support purposes, use of subprocessor services etc. Customers have the option to disable Qualtrics' support access to its account (though support issues may take longer to resolve).

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.

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