

# DATA SHARING AND CONFIDENTIALITY AGREEMENT

## INCLUDING PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY AND SUPPLEMENTAL INFORMATION ABOUT THE AGREEMENT

### 1. PURPOSE

- (a) This Data Sharing and Confidentiality Agreement ("**DSC Agreement**") supplements the Qualtrics, LLC ("**Qualtrics**") Software System agreement ("**Qualtrics Agreement**"), to ensure that the Qualtrics Agreement conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DSC Agreement, a copy of BOCES Parents Bill of Rights for Data Security and Privacy signed by Qualtrics, and the Supplemental Information about the Qualtrics Agreement that is required to be posted on BOCES website.
- (b) To the extent that any terms contained within the Qualtrics Agreement, or any terms contained within any other Agreements attached to and made a part of the Qualtrics Agreement, conflict with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect. In the event that Qualtrics has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Qualtrics Agreement, with respect to Protected Data (as defined below) to the extent that any term of the TOS conflicts with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect.

### 2. DEFINITIONS

Any capitalized term used within this DSC Agreement that is also found in the Qualtrics Agreement will have the same definition as contained within this DSC Agreement.

In addition, as used in this Exhibit:

- (a) "**Student Data**" means personally identifiable information, as defined in Section 2-d, from student records that Qualtrics receives from a Participating Educational Agency pursuant to the DSC Agreement.
- (b) "**Teacher or Principal Data**" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Qualtrics receives from a Participating Educational Agency pursuant to the Qualtrics Agreement.
- (c) "**Protected Data**" means Student Data and/or Teacher or Principal Data to the extent applicable to Qualtrics' Product.
- (d) "**Participating Educational Agency**" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with BOCES, and as a result is licensed to use Qualtrics' Product pursuant to the terms of the Agreement and the Qualtrics Agreement.

### 3. CONFIDENTIALITY OF PROTECTED DATA

- (a) Qualtrics acknowledges that the Protected Data it receives pursuant to the Agreement may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Qualtrics will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) to the extent that such law imposes obligations directly upon Qualtrics as a processor in connection with the service specified in an order form between Qualtrics and a Participating Educational Agency and BOCES policy on data security and privacy in this DSC. Qualtrics acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Qualtrics.

### 4. DATA SECURITY AND PRIVACY PLAN

Qualtrics agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with the BOCES Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by Qualtrics and is set forth below.

Additional elements of Qualtrics' Data Security and Privacy Plan are set forth (1) in the Qualtrics Security and Privacy White Paper Lite ("White Paper"), attached hereto as Exhibit White Paper, and (2) as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with BOCES data security and privacy policy, Qualtrics will follow those processes and policies set forth in the White Paper.
- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Qualtrics Agreement, Qualtrics will have the reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Qualtrics Agreement set forth in the White Paper.
- (c) Qualtrics will comply with all obligations set forth in BOCES "Supplemental Information about the Agreement" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Qualtrics has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Via onboarding and annual security training and as set forth in the White Paper.

- (e) Qualtrics [check one] ☒ will [ ☐ ] will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Qualtrics Agreement. Qualtrics is responsible for breaches of this Agreement caused by its subcontractors.
- (f) Qualtrics will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Qualtrics will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Qualtrics will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the Agreement is terminated or expires, as more fully described in the White Paper.


## 5. **ADDITIONAL STATUTORY AND REGULATORY OBLIGATIONS**

Qualtrics acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Qualtrics Agreement and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Qualtrics in fulfilling one or more of its obligations under the Qualtrics Agreement.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement or to deliver services under the Qualtrics Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Qualtrics using the information to carry out Qualtrics' obligations under the Qualtrics Agreement, unless:
  - (1) the parent or eligible student has provided prior written consent; or
  - (2) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody.
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the Qualtrics Agreement," below.
- (g) Provide notification to BOCES (if configured to be notified via the services) and Participating Educational Agencies of any breach of security resulting in an unauthorized release of Protected Data by Qualtrics or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Qualtrics or its subcontractors or assignees.

## 6. **NOTIFICATION OF BREACH AND UNAUTHORIZED RELEASE**

- (a) Qualtrics shall promptly notify BOCES (if configured to be notified via the services) and the Participating School District of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Qualtrics has discovered or been informed of the breach or unauthorized release.
- (b) Qualtrics will provide such notification to BOCES as and if configured to be notified via the services and via the configured email.
- (c) Qualtrics will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer or designee about the incident, including but not limited to, if readily available: a description of the incident, the date of the incident, the date Qualtrics discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Qualtrics has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Qualtrics representatives who can assist BOCES and the affected Participating Educational Agencies that may have additional questions.
- (d) Qualtrics acknowledges that upon initial notification from Qualtrics, BOCES, as the educational agency with which Qualtrics contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Qualtrics shall not provide this notification to the CPO directly. In the event the CPO contacts Qualtrics directly or requests more information from Qualtrics regarding the incident after having been initially informed of the incident by BOCES, Qualtrics will promptly inform the BOCES Data Protection Officer or designees.
- (e) For any incident affecting only BOCES, Qualtrics will consult directly with the BOCES Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

QUALTRICS, LLC	
By:	
Name:	Mark Creer
Title:	Director, Legal Sales
Date:	14 August 2024

## **PARENTS BILL OF RIGHTS RELATING TO STUDENT DATA**

Clinton-Essex-Warren-Washington BOCES a/k/a Champlain Valley Educational Services (CVES BOCES) is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information will not be sold or released for any commercial purposes;
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by New York State is available for public review at the following website: <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, NYS Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234;
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Network And Systems Coordinator, P.O. Box 455, Plattsburgh, NY 12901; Phone: 518-561-0100 Ext. 343; email (dpo@cves.org). Complaints to the NYS Education Department should be directed to: Privacy Complaint, Chief Privacy Officer, NYS Education Department, 89 Washington Avenue, Albany, NY 12234. Complaints may also be submitted using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

## APPENDIX

### **Supplemental Information Regarding Third-Party Contractors**

In the course of complying with its obligations under the law and providing educational services to District residents, the Clinton-Essex-Warren-Washington BOCES has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

Adopted June 10, 2020

#### **BY THE VENDOR:**

Mark Creer

\_\_\_\_\_  
**Name (Print)**



\_\_\_\_\_  
**Signature**

Director, Legal Sales

\_\_\_\_\_  
**Title**

14 August 2024

\_\_\_\_\_  
**Date**

**Supplemental Information about the Agreement  
between  
BOCES and Qualtrics, LLC**

BOCES has entered into an Agreement ("Agreement") with Qualtrics, LLC ("Qualtrics"), which governs the availability to Participating Educational Agencies of the following Product(s):

Experience Management software and services

Pursuant to the Agreement, Participating Educational Agencies may provide to Qualtrics, and Qualtrics will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

**Exclusive Purpose for which Protected Data will be Used:**

Determined solely by BOCES.

The exclusive purpose for which Qualtrics is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Qualtrics agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the Agreement. Protected Data received by Qualtrics, or any of Qualtrics' subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:**

In the event that Qualtrics engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the Agreement (including any hosting service provider), Qualtrics is responsible for breaches of the Qualtrics Agreement and this Agreement caused by its subcontractors. Qualtrics performs regular reviews of subcontractors and the services they provide. Qualtrics evaluates suppliers based on risk scores.

**Duration of Agreement and Protected Data Upon Expiration:**

- The Agreement commences on October 19, 2024 and expires on October 18, 2025. Following expiration of the Agreement without renewal, or upon termination of the Agreement prior to expiration, Qualtrics will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Qualtrics or its assignees or subcontractors. If (1) self-service export tools are not available and (2) requested by a Participating Educational Agency, Qualtrics will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- Qualtrics agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever beyond its standard data deletion period. Upon request, Qualtrics and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:**


Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Qualtrics, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Qualtrics by following the appeal process in their employing school district's applicable APPR Plan.

**Data Storage and Security Protections:**

Any Protected Data Qualtrics receives will be stored on systems maintained by Qualtrics, or by a subcontractor under the direct control of Qualtrics, in a secure data center facility located within the United States. The measures that Qualtrics will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, encryption at rest, firewalls, and password protection. Qualtrics will comply with the procedures and processes set forth in the White Paper.

**Encryption of Protected Data:**

Qualtrics (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using AES-256.

QUALTRICS, LLC	
By:	
Name:	Mark Creer
Title:	Director, Legal Sales
Date:	14 August 2024

**Exhibit White Paper  
(see attached)**

# Cloud Security and Privacy Framework

Information, Security, Privacy, and Compliance

January 2024

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

#### **Terms & Conditions**

This document contains confidential information regarding Qualtrics' security related operations and policies. There must be a valid confidentiality agreement signed by your organization and Qualtrics, LLC. This document supersedes all previous versions. The Qualtrics security team has created this document to the best of its ability and does not warrant that it is error-free.

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

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

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

<b>Overview of Operations .....</b>	<b>4</b>	<b>Security Governance .....</b>	<b>32</b>
<b>Definitions .....</b>	<b>4</b>	<b>Site Operations.....</b>	<b>34</b>
<b>Service Descriptions .....</b>	<b>5</b>	<b>Corporate Offices .....</b>	<b>34</b>
<b>Locations and Infrastructure .....</b>	<b>7</b>	<b>Data Center Responsibilities (Qualtrics).....</b>	<b>34</b>
<b>People.....</b>	<b>8</b>	<b>Systems Monitoring.....</b>	<b>35</b>
<b>Policies and Procedures .....</b>	<b>9</b>	<b>Third Party Management .....</b>	<b>36</b>
<b>Platform Data .....</b>	<b>10</b>	<b>Training and Awareness .....</b>	<b>37</b>
<b>Control Environment.....</b>	<b>11</b>	<b>Vulnerability Management.....</b>	<b>38</b>
<b>Risk Management.....</b>	<b>11</b>	<b>Using the Service.....</b>	<b>39</b>
<b>Monitoring .....</b>	<b>12</b>	<b>User Controls .....</b>	<b>42</b>
<b>Information and Communications.....</b>	<b>12</b>	<b>Appendix A: US Privacy Regulations.....</b>	<b>44</b>
<b>Control Activities.....</b>	<b>13</b>	<b>Appendix B: EU Privacy Regulations.....</b>	<b>45</b>
<b>Asset Management .....</b>	<b>13</b>	<b>Appendix C: Australian Privacy Regulations .....</b>	<b>46</b>
<b>Business Continuity &amp; Disaster Recovery...</b>	<b>14</b>	<b>Appendix D: Canadian Privacy Regulations .....</b>	<b>47</b>
<b>Backup Management .....</b>	<b>15</b>	<b>Appendix E: California Consumer Privacy Act .....</b>	<b>48</b>
<b>Change Management .....</b>	<b>16</b>	<b>Appendix F: Additional Security and Privacy Framework for XM Discover and Qualtrics Social Connect.....</b>	<b>49</b>
<b>Data Management .....</b>	<b>18</b>	<b>Appendix G: Additional Security and Privacy Framework for XM Journeys .....</b>	<b>53</b>
<b>Endpoint Protection .....</b>	<b>21</b>		
<b>General Operations .....</b>	<b>22</b>		
<b>Identity and Access Management .....</b>	<b>24</b>		
<b>Incident Response.....</b>	<b>26</b>		
<b>Network Operations .....</b>	<b>29</b>		
<b>People Operations.....</b>	<b>31</b>		

# Overview of Operations

Qualtrics is a Software-as-a-Service (SaaS) who provides a platform for creating and distributing online surveys, performing employee evaluations, web site intercepts, and other research services, referred to as the XM Platform. The XM Platform records response data, performs analysis, and produces reports on the data. All services are online and require no downloadable software. Only modern JavaScript-enabled internet browsers and an internet connection are required. Qualtrics offers multiple products for online data collection: CoreXM, Customer Experience, Employee Experience, Product Experience, Brand Experience, and others. Services include providing the products and technical support. Surveys are usually taken online within a web browser, with optional SMS surveys and offline methods available for smartphones/tablets.

## Definitions

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

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

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

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

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

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

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

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

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

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

**“Responses”** mean Data collected from surveys.

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

## Service Descriptions

**Experience  
Design**

qualtrics<sup>XM</sup>

**Experience  
Improvement**

DISCOVER

ENGAGE



**Qualtrics  
DesignXM**

Uncover the products, services, and experiences that customers and employees want next.



**Qualtrics  
CustomerXM**

Decrease churn. Increase Customer Lifetime Value. Reduce cost to serve.



**Qualtrics  
ProductXM**

Improve product market fit. Increase share of wallet. Decrease time to market.



**Qualtrics  
EmployeeXM**

Attract and retain talent. Increase engagement. Improve productivity.



**Qualtrics  
BrandXM**

Acquire new customers. Increase market share. Improve awareness and perception.



**Qualtrics  
XM Services**

Expert designed programs. White-glove implementation and management.



Identify gaps and opportunities



Know where to focus and what to do



Build a culture of action

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

StatsIQ	Stats iQ automatically chooses the right tests and instantly returns results in plain English with powerful visualizations that can be exported to Excel or PowerPoint.
XM Discover	XM Discover is cloud-based software that allows customers to gain insights based on what customers are saying on social media, online reviews, and the contact center interactions.
Social Connect	Social Connect centralizes customer engagements by providing agents one place to manage customer contact, regardless of what channels are used. Agents can see the full history of a case to get a holistic view of every customer's contact, and then respond seamlessly on each customer's preferred channels — without leaving the platform.
XM Journeys	XM Journeys is a next-generation experience orchestration platform. XM Journeys helps companies use contextual data to actively shape experiences in real time that increase customer retention, engagement, and lifetime value.

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

# Locations and Infrastructure

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

FUNCTION	DESCRIPTION
Production Data Centers	<p>Qualtrics utilizes either a combination of both Equinix and Amazon Web Services (AWS) or Amazon Web Services (AWS) exclusively for our production Data storage locations. They are located in the following regions:</p> <ul style="list-style-type: none"> <li>• United States - East (Ashburn, VA)</li> <li>• United States – West (San Jose, CA)</li> <li>• Canada (Montreal, QC [AWS Only])</li> <li>• EMEA (Frankfurt, Germany[AWS Only])</li> <li>• Australia (Sydney, NSW[Moving to AWS Only - Spring 2024])</li> <li>• Singapore (AWS Only)</li> <li>• Japan (Tokyo [AWS Only])</li> <li>• United Kingdom (London [AWS Only])</li> <li>• FedRAMP Environment (San Jose, CA [AWS GovCloud Only])</li> </ul> <p>Data backups and other data elements are stored in Amazon Web Services in the same geographical region where available or through the use of three AWS availability zones.</p>
System Engineering	<p>System Engineering is supported out of the following locations:</p> <ul style="list-style-type: none"> <li>• United States</li> <li>• Ireland</li> <li>• Poland</li> <li>• Mexico</li> <li>• Canada</li> <li>• France</li> <li>• Belgium (Discover Only)</li> <li>• India (Discover Only)</li> <li>• Spain (Discover Only)</li> <li>• Serbia [Ending Spring 2024]</li> <li>• Japan</li> </ul>
Customer Support (QUni)	<p>QUni is supported out of the following locations:</p> <ul style="list-style-type: none"> <li>• United States</li> <li>• Ireland</li> <li>• Australia</li> <li>• Germany (Ending Spring 2024)</li> <li>• Japan</li> <li>• Mexico</li> <li>• Poland</li> <li>• Belgium</li> <li>• United Kingdom</li> <li>• India</li> </ul>
XM Success	<p>XM Success personnel support clients based out of the following locations:</p> <ul style="list-style-type: none"> <li>• United States</li> <li>• Argentina</li> <li>• Australia</li> <li>• Belgium</li> <li>• Canada</li> <li>• Colombia</li> <li>• France</li> <li>• Germany</li> <li>• Hong Kong</li> <li>• India</li> <li>• Ireland</li> <li>• Italy</li> <li>• Japan</li> <li>• Mexico</li> <li>• Netherlands</li> <li>• Singapore</li> <li>• Spain</li> <li>• United Kingdom</li> </ul>

Qualtrics also uses sub-processors in the performance of its services. Details can be found at [www.qualtrics.com/subprocessor-list/](http://www.qualtrics.com/subprocessor-list/).

# People

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

ROLE	RESPONSIBILITIES
Qualtrics University (QUni)	<ul style="list-style-type: none"> <li>• Online / Email / Phone support</li> </ul>
XM Success	<ul style="list-style-type: none"> <li>• Customer specific relationship management and support</li> </ul>
Information Security	<ul style="list-style-type: none"> <li>• Security Alerting and Monitoring</li> <li>• Intrusion Detection</li> <li>• Security Automation</li> <li>• Security Awareness Training</li> <li>• Incident Response</li> </ul>
Fleet Engineering	<ul style="list-style-type: none"> <li>• Physical Hardware Configurations               <ul style="list-style-type: none"> <li>- Server Configurations</li> <li>- Virtualization</li> </ul> </li> <li>• Data Center Management</li> <li>• Disk-level Encryption</li> <li>• Capacity Planning</li> </ul>
Network Operations	<ul style="list-style-type: none"> <li>• Network Device Configuration and Management               <ul style="list-style-type: none"> <li>- Configuration Standards</li> <li>- Access Control Lists</li> </ul> </li> <li>• Network Access</li> </ul>
System Engineers / Quality Engineers	<ul style="list-style-type: none"> <li>• New Code Development, Hotfixes</li> <li>• Quality Control</li> <li>• Performance Monitoring</li> </ul>
Data Engineers	<ul style="list-style-type: none"> <li>• Database Configuration and Management</li> <li>• Data Backups (availability)</li> </ul>
Platform Security	<ul style="list-style-type: none"> <li>• Define Platform Security Requirements</li> <li>• Vulnerability Management</li> <li>• Penetration Testing</li> <li>• Security Champion Program</li> </ul>
IT	<ul style="list-style-type: none"> <li>• Corporate Infrastructure</li> <li>• Corporate Wireless Networks</li> <li>• Workstation Management</li> </ul>
Security Assurance	<ul style="list-style-type: none"> <li>• Vendor Risk Assessments</li> <li>• Security Compliance (external audits)</li> <li>• Customer Compliance programs</li> </ul>
People Operations	<ul style="list-style-type: none"> <li>• Employee Onboarding / Offboarding</li> <li>• Awareness Training</li> </ul>
Legal	<ul style="list-style-type: none"> <li>• Contract Management</li> <li>• Privacy</li> <li>• Incident Response</li> <li>• General Legal Support</li> </ul>

# Policies and Procedures

Qualtrics maintains policies and procedures based upon a variety of security frameworks including National Institute of Technology Special Publication 800-53 Rev. 5 International Organization for Standardization 27001, and FedRAMP. Control families include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment, Authorization, and Monitoring
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environment Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Supply Chain Risk Management

Policy and procedure documents are internal only and not released. The sections that follow provide an overview of the content of our policy and procedure documents.

## 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 in a multi-tenant data center and in the data center chosen by the Customer in the applicable order form. While Data is hosted within the region where the Customer's primary data center resides, Data may be transferred and processed outside the data center region to comply with Customer requests or instructions (e.g., support purposes, use of sub-processor services) or as necessary to provide the Cloud Service. In all data centers, Qualtrics operates and is responsible for all system and developed software.

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

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

Qualtrics does not classify Data into sub-categories of confidential information. All Data is treated as confidential and is processed equally regardless of their content.

# 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 any control deficiencies identified in internal and/or external audit reports.

# Risk Management

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

The following key principles outline Qualtrics' approach to risk management and policies:

1. The board and senior officers have responsibility for overseeing risk management within the company as a whole.
2. The senior management team supports, advises, and implements policies approved by the board and officers.
3. Management recognizes and weighs the financial and non-financial implications of the risks.
4. Managers are responsible for encouraging good risk management practice within their department(s).
5. Key risk indicators will be identified and closely monitored on a regular basis.

## RISK ASSESSMENT

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

## CONTROL IMPLEMENTATION

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

## INTERNAL AND EXTERNAL AUDIT

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

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

## REMEDIATION PLANS

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

## Monitoring

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

## Information and Communications

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

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

# Control Activities

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

## Asset Management

### **INVENTORY OF ASSETS**

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

### **ASSET OWNERSHIP**

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

### **ASSET MOVEMENT**

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

### **BASELINE HARDENING STANDARDS**

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

### **TIME SYNCHRONIZATION**

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

# Business Continuity & Disaster Recovery

## BUSINESS CONTINUITY PLAN

Qualtrics has an extensive Business Continuity Plan (BCP) in event of a disaster. Though details of the plan are internal only, below is a summary of how key business operations will operate following a disaster.

- **Purpose:** The purpose of this business continuity plan is to ensure prompt and complete return to normalcy in the event of a service-affecting disaster.
- **Goals and Objectives:** The objectives of this plan are to ensure that, in the event of a disaster all necessary support functions of the organization continue without undue delay. Data integrity and availability along with necessary support functions within the organization enable Qualtrics to maintain a trusting relationship with our customers even in times of disasters.
- **Remediation:** Testing the BCP is performed at least twice per year. Any significant findings are collected, and a report is produced for Engineering 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 of activities:

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

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

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

## BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN TESTING

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

# Backup Management

This section pertains to Data in the Services, not Qualtrics internal company retention procedures. Customers must back up their Data for use in case of accidental deletion/modification caused by one of their Authorized Users or for alignment with their own archive/data retention policies.

## **BACKUP CONFIGURATION**

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

## **SYSTEM REDUNDANCY**

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

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

## **BACKUP DATA RETENTION**

As between Qualtrics and its Customers, Customers own and control their Data, and, therefore, Customers are responsible for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of their Data. They are also responsible for backups (there are numerous download formats and mechanisms available) and retaining the backup according to their own retention policy. This is highly recommended as Qualtrics is under no obligation to restore lost Data caused by the Customer's own negligence. Depending on how active Data is deleted, it may be possible for the Authorized User to undelete it using a feature in the software. Once Data is permanently deleted, then the Authorized User must restore from a personal backup.

The data backups created by Qualtrics are retained for up to 90 days. Restoration from these backup datasets is for disaster recovery only. The backups are electronic (no tapes) and stored in an alternate data center in the same region or by making use of three AWS Availability Zones.

Data may be deleted by the Authorized User at any time using the standard web interface. It is incumbent upon the Customer to determine its own data retention obligations as they relate to their company's policy or legal obligations.

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

# Change Management

## DEVELOPMENT METHODOLOGY

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

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

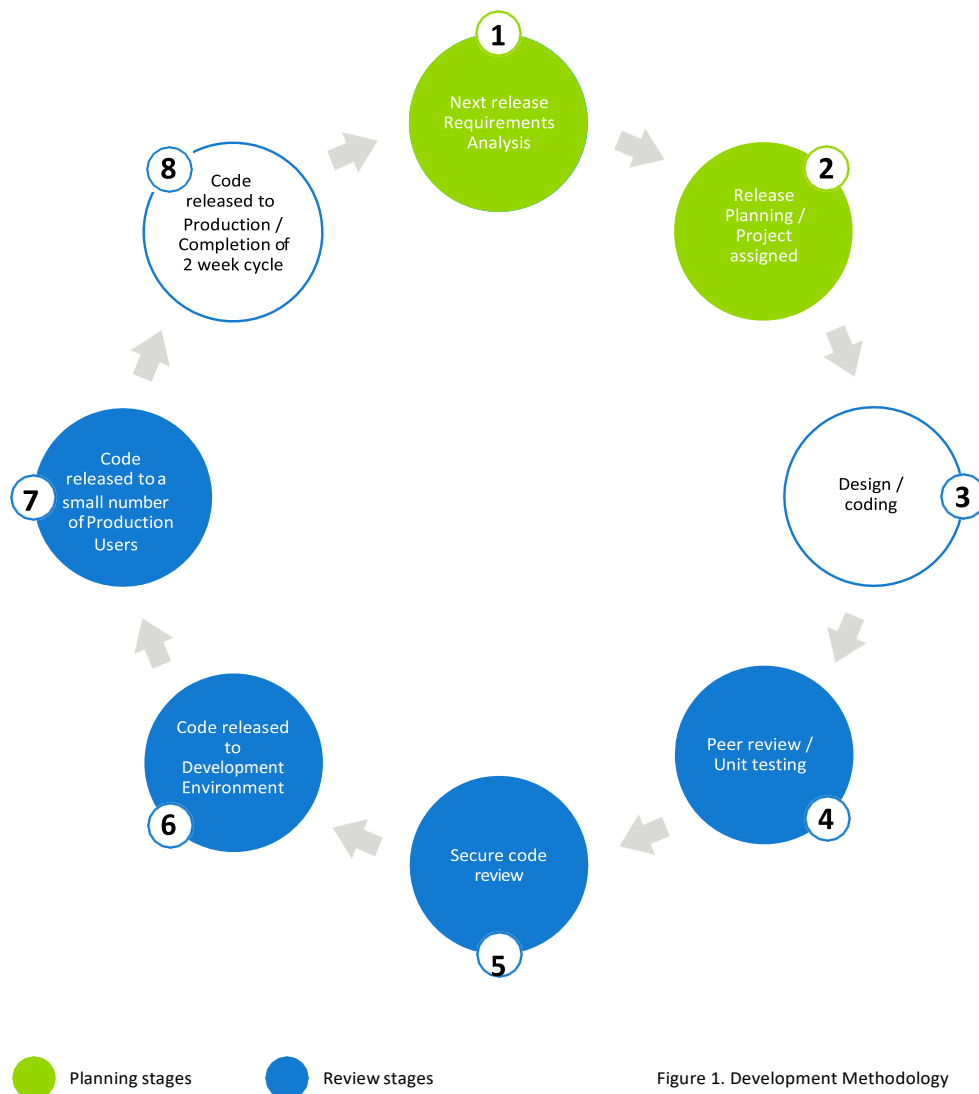


Figure 1. Development Methodology

## CHANGE MANAGEMENT

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

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

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

## APPLICATION CHANGE MANAGEMENT

### *Staging Environment*

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

### *Code Reviews*

Application code review is mandatory for all source code changes. Programmers work individually or in pairs developing new code. As the end of each cycle approaches, code is peer-reviewed and tested in a staging environment which is maintained separately from the production environment. Issues identified in the code review process must be addressed prior to moving to the next step.

### *Static Code Analysis*

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

## INFRASTRUCTURE CHANGE MANAGEMENT

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

## SEGREGATION OF DUTIES

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

## SOURCE CODE MANAGEMENT

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

## PRODUCT UPDATES

Qualtrics provides information on major releases via [www.qualtrics.com/product-updates](http://www.qualtrics.com/product-updates).

# Data Management

## DATA CLASSIFICATION

Customers own and control all Data entered in or collected by the Customer using the Qualtrics Services.

Qualtrics does not classify this Data.

## TYPES OF DATA COLLECTED

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

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

## SENSITIVE DATA POLICY

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

## DATA STORAGE

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

Access to Data requires direct ownership (the user who created the survey) or implied access (e.g., Brand Administrator or another Authorized 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 center region to comply with Customer requests or instructions (e.g., support purposes, use of sub-processor services, or as strictly necessary to provide the Cloud Service).

## ENCRYPTION OF DATA IN TRANSIT

All access to Qualtrics front-end Services is via Hypertext Transfer Protocol Secure (HTTPS) and enforces HTTP Strict Transport Security (HSTS). The platform enforces Transport Layer Security (TLS) v1.2 at a minimum for all interaction with the platform and inside the platform through our service-to-service encryption. Access to the back-end services using the Qualtrics API supports TLS v1.2 or greater. 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.

## ENCRYPTION KEY MANAGEMENT

Encryption keys are stored within a software vault where they are encrypted with key encrypting keys of equivalent strength. Keys are rotated annually or upon a qualifying event.

## ENCRYPTED BACKUPS

Data backups are encrypted using AES 256-bit encryption.

## PASSWORD ENCRYPTION

Passwords are never passed or stored in plain text. Passwords are hashed and salted using an industry accepted hashing algorithm.

## EMAIL SECURITY

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

## DATA ISOLATION ENCRYPTION (Opt-in Feature)

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

## BRING YOUR OWN KEY (BYOK) (Opt-in Feature)

As part of the data isolation feature, Qualtrics supports BYOK. BYOK allows a client to effectively destroy or deny access to their data in Qualtrics' possession. Customers provide Qualtrics access to an [AWS KMS master key](#) to create and use [data keys](#). Qualtrics uses the Customer controlled and owned master key for data key encryption and decryption. If a client declines Qualtrics access to their master key, Qualtrics can ultimately no longer decrypt or decipher that client's data. For additional information on Data Isolation (and BYOK), a Data Isolation Overview document can be requested from your Qualtrics point of contact.

## DATA USED IN TEST ENVIRONMENTS

Customer data is never used in the test environment.

## DATA MODIFICATION

A survey response may be edited if the Authorized User has been granted appropriate permissions by the Customer's Brand Administrator (this is controlled with the survey permissions, namely the "Edit Survey Responses" option). This enables the Authorized User to correct errors and manage data subject requests and other privacy law obligations.

## DATA DELETION

As the data controller, the Customer and its Authorized Users solely determine what Data to delete and when to delete it. Qualtrics provides the platform. An Authorized User with the proper permissions (as set by the Brand Administrator) may:

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

These deletion (and modification) options enable the Customer to manage certain privacy law obligations including data subject requests. Depending on the access levels of the Authorized User who deletes data, there is a soft or hard delete option within the platform. When a soft delete is performed (e.g., deletion by a non-Brand Administrator), Data resides in production for up to 90 days before the 90-day period for removal from backups commences. Some features support customizable retention periods after a soft deletion. In those cases data will be deleted in accordance with the customer's configuration or explicit hard delete action.

In the instance of a soft delete, the Brand Administrator has the ability to undelete Data within the soft deletion period. This is important, as an Authorized User could accidentally or intentionally delete Data. In the same interface, the Data may be undeleted or permanently deleted.

## DATA REMOVAL - LEAVING THE PLATFORM

Because Customers are in control of their Data, Qualtrics encourages Customers to export and delete their Data from Qualtrics prior to terminating their license to use the platform. After the conclusion of the contract period, the Customer will no longer be able to access any Data remaining on the platform. Qualtrics then will delete any remaining Data in accordance with applicable law and contractual obligations.

Customers requesting confirmation of Data deletion should make such request 180 days after expiry of their contract.

## DATA LOSS PREVENTION PROGRAM

Qualtrics has established a program to monitor and alert on unauthorized data moves. Controls in our corporate and production environments include the following:

### Corporate:

- Website filtering on the network.
- USB blocking by default on end user workstations.
- Email filtering rules to block sensitive data.

### Production:

- Access to the production environment is provisioned based on the principles of "least privilege" and "need to know".
- A jump server is in place to access the production environment with detailed logging on specific commands that would be used to move data. Logs are sent to our SIEM, which notifies our Security Operations Center (SOC) if relevant commands are run.
- Direct database logging and monitoring (by data engineering teams and our SOC).
- Database monitoring for spikes in utilization that would result from large data reads.

## DISPOSAL OF MEDIA

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

# Endpoint Protection

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

## **DESKTOP POLICIES**

Each component of our infrastructure (operating systems, desktops, routers, servers), both internal and in the data centers, have baselines that include security settings and default applications. This section applies to the desktops and laptops (collectively, Workstations) used by Qualtrics employees.

## **OPERATING SYSTEMS**

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

## **FULL DISK ENCRYPTION**

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

## **APPLICATIONS AND COMPANY DATA**

The entire desktop environment is standardized using a secure configuration and basic applications as required by job function. This basic setup allows employees to be mobile as users are not necessarily tied to specific devices—though each employee is assigned a device. Internal systems hold some accounting and finance information, but no Customer Data. Instant Messaging is restricted to internal company communications. Nearly all software used by Qualtrics employees during the normal course of business is SaaS/ASP-based.

## **CLEAN DESK POLICY**

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

## **MOBILE POLICY**

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

## General Operations

The Qualtrics online Privacy Statement details how Qualtrics processes personal information it has collected as a data controller and can be found at [www.qualtrics.com/privacy-statement/](http://www.qualtrics.com/privacy-statement/). Please note, this Privacy Statement does not apply to personal data collected by the Customer when using the Qualtrics services. In addition, the Terms of Service ([www.qualtrics.com/terms-of-service/](http://www.qualtrics.com/terms-of-service/)) state the terms and conditions which govern the use of the Qualtrics services, including links to our acceptable-use policies and service-specific terms.

Qualtrics reserves the right to disable any Authorized User account suspected of violating our Terms of Service or other policies. This includes uploading harmful or hateful content (except for valid research purposes), using the Services to “phish” or “spam”, or violating the Terms of Service or terms of an executed order form and/or agreement between Qualtrics and Customer (whichever is applicable).

While Qualtrics cannot prevent Customers from entering any specific type of information, prudence and common sense apply. Research software should not be used to store sensitive information, such as financial details, credit card numbers, social security numbers, criminal records, or genetic information; unless de-identified. When collecting special categories of data, or sensitive personal data, Customers should only do so in compliance with applicable data protection laws and Customers should satisfy themselves that the technical and organizational measures implemented by Qualtrics are sufficient for the types of data they wish to collect.

### CUSTOMER SUPPORT

Qualtrics University (QUni or technical support) staff may ask for personal information before accessing an Authorized User’s account to confirm the Authorized User’s identity. However, they will never ask for an Authorized User’s password. Passwords are salted-hashed values and not viewable by any Qualtrics employee. With the Authorized User’s permission, QUni may access an account to assist in supporting the Authorized User or to diagnose a problem the Customer is experiencing. Such access may be fully disabled by the Brand Administrator across the entire brand but doing so results in no Authorized Users being able to avail of such assistance and may result in decreased support quality.

### WEB PRACTICES

Qualtrics collects and analyzes aggregate information of visitors, including the domain name, visited surveys, referring URLs, and other publicly available information. We use this information to help improve our website and services, and to customize the content of our pages for each visitor. In addition, Qualtrics reads browser languages and settings in order to customize surveys for Respondents.

### ANTI-CORRUPTION AND ANTI-BRIBERY

The Qualtrics organization has been built on transparency and trust. Qualtrics has implemented internal policies including the Code of Ethics and Business Conduct, which contain strict anti-bribery, anti-fraud, and anti-corruption policies, to enable our employees to conduct all business ethically, not to send or receive bribes, or to otherwise participate in corrupt activities. Qualtrics requires all employees to accept and comply with the Code of Ethics and Business Conduct upon hire, and at least annually thereafter.

## **BILLING PROCESSES**

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

## **PROTECTING CHILDREN**

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

## **INSURANCE**

Qualtrics maintains A- or better insurance for industry standard policies and coverages. See <https://www.qualtrics.com/evidence-of-insurance/> for details.

# 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 principles of least privilege and need to know 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 XM Success), engineering teams for maintenance and 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 the employee's role, it is revoked. This includes termination of employment as well as changes to roles or responsibilities in the company. The uncoupling process is completed within 24 hours of a role change, or immediately at employment termination. During such an event, a ticket gets created by a manager or HR employee, and emails get sent to various departments. The ticket is managed by HR to ensure that all actions are being performed during the change/termination (such as access to systems and buildings).

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

## **ACCESS AUTHENTICATION**

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

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

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

## **USER ACCESS REVIEWS**

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

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

## **PASSWORD POLICY**

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

- Passwords must be a minimum password complexity of 12 characters and must contain a combination of letters, numbers, and symbols based on available system functionality.
- Password maximum lifetime is restricted to 60 days.
- Passwords cannot be reused for at least 12 generations.
- Account lockout settings are enforced after a number of consecutive invalid login attempts and automatically lock the account after the number of unsuccessful attempts is exceeded.
- Passwords are checked against commonly used passwords.

## **MULTI-FACTOR AUTHENTICATION**

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

## **VIRTUAL PRIVATE NETWORK (VPN)**

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

## **SECRET STORAGE**

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

# Incident Response

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

## **INCIDENT RESPONSE PLAN**

Qualtrics has developed Incident Response policies and procedures to ensure the integrity, confidentiality, and availability of the Data. These policies and procedures are consistent with applicable laws, 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.
- Any event that triggers privacy notification obligations, even if such an event is not due to Qualtrics' actions or inactions.

Incident Response Plan includes the following lifecycle steps.

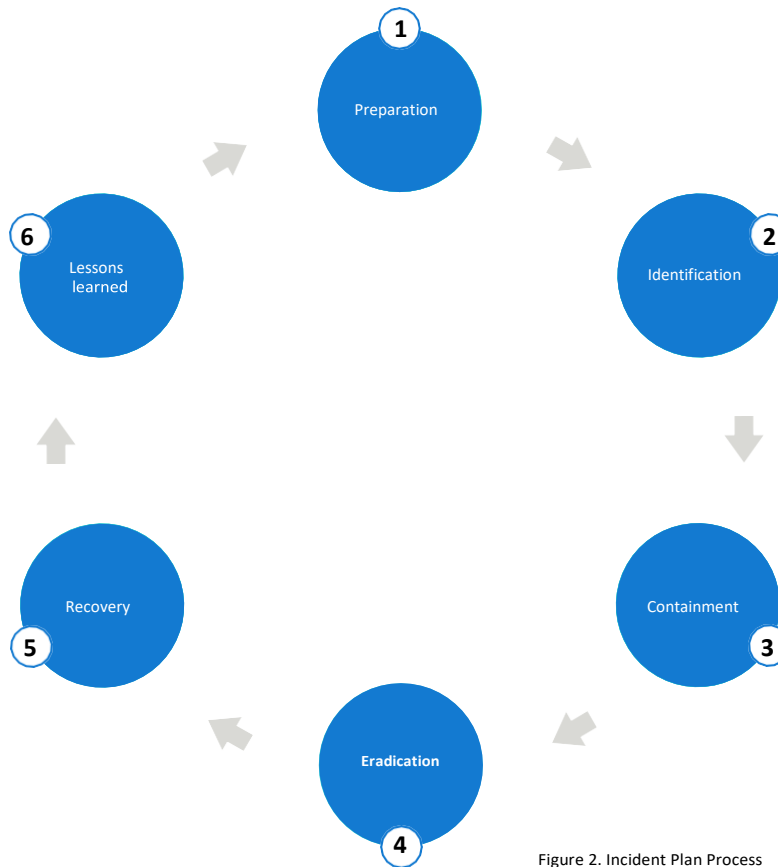


Figure 2. Incident Plan Process

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

## **INCIDENT RESPONSE PLAN TESTING**

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

## **SECURITY OPERATIONS CENTER PERSONNEL**

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

Customers will be notified of any Incident in accordance with their contract with Qualtrics. The Brand Administrator is the key point of contact for all notifications and will be kept aware of the investigation and remediation efforts. If customers want to nominate a specific security contact, they can do so within Organizational Settings on the platform. See – <https://www.qualtrics.com/support/survey-platform/sp-administration/organization-settings/>.

## **INCIDENT REPORTING CONTACT INFORMATION**

If you suspect a security or privacy breach/incident, please contact Qualtrics by contacting your account representative or speak with a support representative at <https://www.qualtrics.com/support/>.

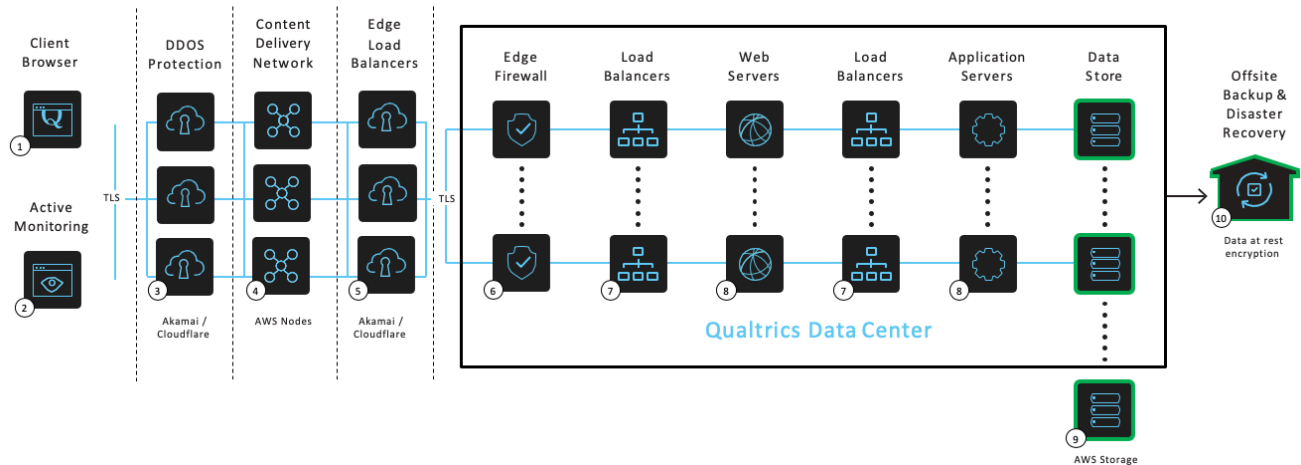
## **DATA BREACH NOTIFICATION REQUIREMENTS**

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

# Network Operations

## DATA FLOW

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



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

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

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

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

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

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

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

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

**9 Data Store** – Databases designed for scale and performance for both data collection and reporting. Data stores and responses are encrypted using AES-256 with Qualtrics managed keys

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

This multi-tiered architecture has multiple layers of hardware and software security to ensure that no device/user can be inserted into the communication channel. Email may be configured to use opportunistic TLS to send encrypted messages to an external email server or as a relay to the Customer's email server. Qualtrics leverages a Web Application Firewall to prevent DDoS attacks. The Qualtrics Security Operations Center provides 24/7 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 1.2 or greater for all interaction with the platform. Access to services using the Qualtrics API supports TLS v1.2 or greater. Data is processed by application servers and sent to database servers for storage.

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

Authorized Users access the Qualtrics platform with login credentials. 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 Authorized Users and the password policy.

### **WEB APPLICATION FIREWALL**

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

### **NETWORK POLICY ENFORCEMENT POINTS**

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

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

### **NETWORK SEGMENTATION**

Qualtrics systems consist of three logically and physically separate networks: corporate, development/test, and production networks. The corporate network supports internal business functions and the authentication mechanism is completely separate from the development/test and production environments. The development/test network is designed to support software development and quality engineering. No wireless networks are attached to this network.

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

### **WIRELESS NETWORKS**

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

# People Operations

All new hires are held to rigorous standards, must have the required qualifications for their role, and must complete background checks (as permitted by applicable laws). Qualtrics is an equal opportunity employer.

## BACKGROUND SCREENING

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

	GLOBAL	UNITED STATES
Education Verification	•	•
Employment Verification	•	•
Criminal Check (where allowed by law)	•	•
Global Watchlist (includes OFAC Search, Politically Exposed [PEP], Prohibited Parties Search)	•	•
Adverse Media	•	•
SSN Trace		•
DOJ Sex Offender		•

## EMPLOYEE AGREEMENTS

Upon hire, all Qualtrics employees are required to sign an employment agreement containing privacy and confidentiality obligations that specifically address the risks of dealing with confidential information, including Customer accounts and Data. Any employee found to have violated these requirements will face internal disciplinary action, with possible legal consequences.

## DISCIPLINARY PROCESS

Employees alleged to have violated Qualtrics information security policies are investigated. Depending on the severity of the allegations and results of the investigation, Qualtrics may suspend the employee's access to the affected systems and/or take disciplinary action, up to and including termination of employment. Following the investigation, notification occurs to the appropriate internal parties regarding results of the investigation and any disciplinary action taken.

# Security Governance

## INFORMATION SECURITY MANAGEMENT SYSTEM

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

## SECURITY GOVERNANCE COMMITTEE

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

- Overseeing creation, implementation and updates of security and privacy policies and procedures.
- Overseeing security and privacy risk assessments and audits.
- Monitoring compliance with the ISMS.

## SECURITY CERTIFICATIONS

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

 <p>SOC2 Type II Security, Confidentiality, Availability</p>	 <p>HITRUST CSF v9.3</p>	 <p>FedRAMP FedRAMP Government Data Standards (Moderate)</p>	
 <p>ISO 27701 Data Privacy Controls</p>	 <p>ISO 27001 Security Management Controls</p>	 <p>ISO 27017 Information Technology Security Techniques</p>	 <p>ISO 27018 Information Technology Security Techniques</p>
 <p>IRAP PROTECTED- Level Controls</p>	 <p>CYBER ESSENTIALS Cyber Threat Protection</p>	 <p>TISAX</p>	

Qualtrics makes copies of select certifications and security documents available to current and future customers. Current customers may download copies of the most recent versions from the Security Document Center (<https://support-portal.qualtrics.com/document-center>). Future customers may request copies of available documents from the Qualtrics Trust Center (<https://www.qualtrics.com/trust-center/>). Note that some documents require future customers to have a confidentiality agreement in place before sharing.

## **FIPS SECURITY REQUIREMENTS**

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

## Site Operations

Qualtrics is responsible for the physical security controls at its corporate offices, and components of physical security controls within the co-location data centers. Physical security controls of the third-party data centers are the responsibility of the data center service provider. The controls are monitored annually through onsite visits where possible 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. Where permitted by law, video surveillance is recorded and maintained for a minimum of 30 days to allow for a review.

### VISITOR ACCESS

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

## Data Center Responsibilities (Qualtrics)

### DATA CENTERS

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

In general, all data centers utilized by Qualtrics:

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

### PROVISIONING PHYSICAL ACCESS

Physical access to colocation data centers is controlled by Qualtrics and restricted to a limited number of employees and includes the locked cage that houses the hardware used to provide the Services. Those employees do not have direct access to Data. Access to the data center is managed by Fleet Engineering. They are responsible for provisioning and de-provisioning physical access. Our third-party data center provider (AWS) does not permit physical access to their facilities.

### PERIODIC REVIEW OF PHYSICAL ACCESS

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

# Systems Monitoring

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

## SECURITY MONITORING

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

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

## INTRUSION DETECTION

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

## PERFORMANCE MONITORING

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

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

Customers can monitor system status at [status.qualtrics.com](https://status.qualtrics.com).

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

## LOG RETENTION & PROTECTION

System and performance logs are sent to a SIEM for long term storage. The SIEM is configured to “Write Once, Read Many” to prevent logs from being tampered. Log files typically contain requestor IP address, protocol, request, result, and other info. Real-time dashboards provide insight into the log files using advanced analysis techniques. No response data is captured in log files. Full logs are internal only and unavailable to Customers. A subset of logs are made available to Customers in the platform or via API.

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

# Third Party Management

## THIRD PARTY DUE DILIGENCE

To mitigate risk to Qualtrics and Customers, the Procurement, Security Assurance and Legal Vendor teams perform initial and regular reviews of suppliers and partners (collectively referred to as “suppliers”) including any sub-processors. These reviews are based on the services they provide to and for Qualtrics. The Third-Party Risk Assessment process evaluates suppliers using a questionnaire based on industry standards. The questionnaire covers control areas including, but not limited to; Information Security, Logical Access, Vulnerability Management, Change Management, Data Security and Data Privacy. Each supplier receives a risk score based on the answers provided to the questionnaire. This risk score and the applicable use case are evaluated, and the supplier is assigned a risk rating from Low to High risk.

Suppliers are subject to reassessment on a defined cadence based on their overall risk rating. If a gap is identified, Qualtrics will evaluate the severity of the gap and where appropriate require the Vendor to create a remediation plan with a defined timeframe. Failure to implement/ comply with this remediation plan may result in Qualtrics stopping all business with the Vendor.

## ANNUAL SUB-PROCESSOR AUDIT REPORT REVIEW

Key suppliers that support Qualtrics' infrastructure are required to hold and maintain independent security audit reports (for example SOC 2 Type II or ISO 27001). Audit reports are reviewed annually to ensure ongoing compliance with contractual obligations to achieve availability, confidentiality, security, and privacy commitments. Data centers must maintain independent security audit reports (for example SOC 2 Type II or ISO 27001) to validate that physical and environmental controls are in place and operating as designed. These audit reports and the physical and environmental controls are also reviewed annually. In addition to these audits, Qualtrics personnel may visit those data centers where company owned assets are located.

## THIRD PARTY AGREEMENTS

The Qualtrics Legal team ensures information security requirements are captured as part of service level agreements with new suppliers. Third party service providers who may have physical or logical access to the Qualtrics platform, Qualtrics personal data or customer data are required to acknowledge and agree to confidentiality, availability, data security and privacy requirements.

# Training and Awareness

## GENERAL SECURITY AND PRIVACY AWARENESS TRAINING

Qualtrics employees are formally trained on company policies and security and privacy practices. This training occurs at the time of hire and at least annually thereafter, through in-person or online training for remote employees. In addition to the trainings, regular updates are provided throughout the year through email, newsletter, intranet postings, and regular company meetings. All employees are instructed to immediately report possible security or privacy incidents to Information Security. The Qualtrics employee handbook includes policies and guidance on the following topics:

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

## SECURITY TRAINING FOR ENGINEERS

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

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

# Vulnerability Management

## **VULNERABILITY ASSESSMENT, TRIAGE, AND RESOLUTION**

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

Remediation plans are developed as necessary to address critical risk vulnerabilities as soon as possible, but within 14 days, high risk vulnerabilities within 30 days, moderate risk vulnerabilities within 90 days and low risk vulnerabilities within 180 days, except in extenuating circumstances.

## **ANTI-MALWARE PROTECTION**

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

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

## **PATCH MANAGEMENT**

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

## **PENETRATION TESTING**

External security assessments are performed by an independent third-party. Penetration tests against the production environment are performed annually. Remediation plans are documented to address findings from the report. Findings and remediation plans are presented to the Security Governance Committee and tracked until they've been addressed. Summary results of external penetration tests are available in the Security Document Center or Trust Center.

Qualtrics maintains an internal penetration team that is continuously testing elements of the applications looking for bugs. Similar to the 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 definitions regularly and scan the environment to identify missing patches and other misconfigurations. Patches are applied based on the overall risk rating. Vulnerability scan reports are internal only and not released.

# Using the Service

This section is specific to Customers and their Authorized Users using the Qualtrics platform.

## BRAND ROLES

These roles are found within Qualtrics products. More details may be found at [www.qualtrics.com/support](http://www.qualtrics.com/support).

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

## ACCOUNT ACCESS CONTROL FOR THE SERVICE

- **The Qualtrics Authorized 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 Authorized Users with a Division Administrator.
- **Collaboration:** Individual surveys may be collaborated (or shared) with other Authorized Users or Groups. When collaborating, an Authorized User can specify which permissions other Authorized Users or Group Members should have, including access to view associated Data. Access to collaboration functions may be restricted on a per-Authorized 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 Authorized User account within the Brand (the audit log will show that login).

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

## PASSWORD POLICIES FOR THE SERVICES

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

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

- **Failed Attempts:** In order to block unauthorized access through password guessing, accounts are disabled after six invalid login attempts. Once an account has been deactivated, the account stays deactivated for ten minutes (and reset each time a new login attempt is performed). The Brand Administrator may also reactivate the account.
- **Password Complexity:** Settings for length, complexity (non-alpha characters), and periodic password expiration are available at the Brand level. For more complex password requirements, SSO integration is recommended. A unique error message may be sent when a password doesn't meet the stated requirements.
- **Password Expiration:** Settings for expiration are defined within the organization settings. The configuration is defined in number of days. A unique error message may be sent when a password doesn't meet the stated requirements.
- **Forgotten Password Policy:** If a user forgets their password or makes more than six invalid login attempts (causing their account to become deactivated), they may call Qualtrics support for help. There is also an optional self-service password reset option that sends an email with a link to create a new password.
- **Single Sign-On:** SSO allows Customers to better control user management (additions/deletions) from the Customer's directory service, directly linked to the Qualtrics authentication service. Industry standard protocols are supported, including LDAP, CAS (Central Authentication Service), Google OAuth 2.0, Token, Facebook, and Shibboleth (SAML).

These settings are controlled within the Advance Security Tab.

See - <https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/> for more details.

## SURVEY SECURITY AND USAGE

There are several ways to protect surveys from being "stuffed" or from being taken by the wrong respondent. For example, surveys may be sent to specific individuals, require a password, or be taken only by Customer employees etc.

Full details are available on the Qualtrics support website [www.qualtrics.com/support](http://www.qualtrics.com/support). Authorized Users determine who should take the survey and what content should be collected. Survey links may be posted on a webpage, sent in email, or printed on paper and delivered via certified mail.

Brand Administrators control the brand, including Authorized Users and their permissions, survey design, distribution, collected Data, etc. There is an option to require approval before a survey is distributed, thereby enabling an Authorized User to review a survey before it is sent. Qualtrics is not responsible for any Data lost or stolen due to negligent Authorized Users.

## **PRIVACY IMPACT ASSESSMENT**

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

Qualtrics performs its own PIAs based upon the NIST 800-53 standard, and as required by applicable law. Any PIA conducted is internal only. Qualtrics will provide reasonable assistance to customers to enable customers to perform their own PIAs in accordance with Qualtrics' contractual obligations.

# User Controls

The Qualtrics platform is a self-service platform and as such, there are a number of controls that Qualtrics' Customers should implement to support their own 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. See - <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. See - <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 configure multi-factor authentication (MFA). See - <https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/>

**Audit Logs:** Customers that have access to the Security tab linked above also have access to an activity log. The platform also allows for these logs to be pulled from the system via an API call to the platform. Information on how to get activity logs is located on the Qualtrics API page. See - <https://api.qualtrics.com/api-reference/YXBpOjYwOTEy-audits>

**User Provisioning/Deprovisioning:** Customers are responsible for creating valid user accounts within the application. Qualtrics creates an initial customer administrator account (the Brand Administrator(s)), 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 Allowlists:** Customers can set up the application to limit which IP addresses are allowed to access their instance. Customers are responsible for maintaining this list. See here - <https://www.qualtrics.com/support/survey-platform/sp-administration/managing-users/user-permissions/>

**Data Storage:** Customers are responsible for selecting the data center where their data will be stored on the applicable order form.

**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, such as:

- Within the Platform: [www.qualtrics.com/support/survey-platform/data-and-analysis-module/data/download-data/export-options/](https://www.qualtrics.com/support/survey-platform/data-and-analysis-module/data/download-data/export-options/)
- API: [api.qualtrics.com/](https://api.qualtrics.com/)

**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 and should not be collected as part of a question or in the response.

## Appendix A: US Privacy Regulations

### **HEALTH INSURANCE PORTABILITY AND ACCESSIBILITY ACT (HIPAA)**

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

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

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

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

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

### **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT**

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

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

## Appendix B: EU Privacy Regulations

### GENERAL DATA PROTECTION REGULATION

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 organizations that fall within the material and territorial scope of GDPR.

Qualtrics enables its Customers to be GDPR compliant by providing the necessary documents and tools to enable the Customer to fulfill the Customer's obligations as a data controller. Several sections in this Cloud Security and Privacy Framework describe the tools provided by Qualtrics, including authentication and access, response editing and deletion, etc.

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 Authorized Users to modify and delete individual data points.
- enable Authorized Users to modify and delete complete survey responses.
- enable Authorized Users to modify and delete the entire project (responses and survey definitions).
- provide security-related documentation that describes the processes and procedures for safeguarding the Data (certain documents subject to the execution of confidentiality agreements).

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

## Appendix C: Australian Privacy Regulations

### AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL

The Australian Government, through the Australian Cyber Security Centre (ACSC), provides an Information Security Manual (ISM) that outlines key principles and security controls to help safeguard Australian Government IT systems.

The Qualtrics XM Platform is periodically subjected to an independent assessment against the PROTECTED-level security controls of Australian Government ISM under the Information Security Registered Assessors Program (IRAP). This helps Australian Government security officers perform periodic threat/risk assessments (TRAs) and to make risk-informed decisions about how to handle their organizations' data.

### AUSTRALIA FEDERAL PRIVACY ACT

The Privacy Act 1988 (Cth) applies to federal government agencies and private organizations that:

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

The Privacy Act includes thirteen Australian Privacy Principles (APPs) that set out binding standards and obligations APP entities must meet in relation to handling, holding, accessing, collecting, using, disclosing, storing, and correcting personal information. As the Customer, an organization will need to consider how the principles of APP apply to their processing of personal data using the Qualtrics platform

Qualtrics generally meets or exceeds the APPs that relate to its processing of Data—specifically, only using Data to fulfil its obligations as related to the Services and applicable agreements, maintaining a high level of security, and having a transparent privacy policy. Qualtrics' privacy statement is available at [www.qualtrics.com/privacy-statement/](http://www.qualtrics.com/privacy-statement/).

### FURTHER READING

Further details on how the Qualtrics XM Platform meets Australian Government regulations are available at [www.qualtrics.com/au/government/](http://www.qualtrics.com/au/government/)

## Appendix D: Canadian Privacy Regulations

### PRIVACY ACT OF 1983

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

### PIPEDA: PERSONAL INFORMATION PROTECTION AND ELECTRONICS DOCUMENTS ACT OF 2000

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

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

PIPEDA has ten Fair Information Principles ("Principles"), listed below. Qualtrics has completed a self-certification of the Principles. Customers, as controllers of any Data collected using the Qualtrics Services, will need to perform their own assessments and abide by Fair Information Principles.

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

## Appendix E: California Consumer Privacy Act

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

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

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

# Appendix F: Additional Security and Privacy Framework for XM Discover and Qualtrics Social Connect

XM Discover and Qualtrics Social Connect offerings follow the same or similar practices and principles as stated above with the following exceptions.

## Locations and Infrastructure

XM Discover and Qualtrics Social Connect are hosted by third-party data centers that are audited using industry best practices. The infrastructures are hosted in Amazon Web Services, IBM Cloud and Unix Solutions. These production data centers are located in the following regions:

- United States (East and South)
- Canada
- EMEA (Germany and Belgium)

## DATA CENTERS

XM Discover uses IBM Cloud and AWS as data center providers. For IBM, XM Discover and Social Connect customers can request the latest SOC 1, SOC 2, and SOC 3 reports on the infrastructure and data centers. Our data center provider's ISO 27001:2013, PCI attestation of compliance, and HIPAA bridge letters are also available upon request.

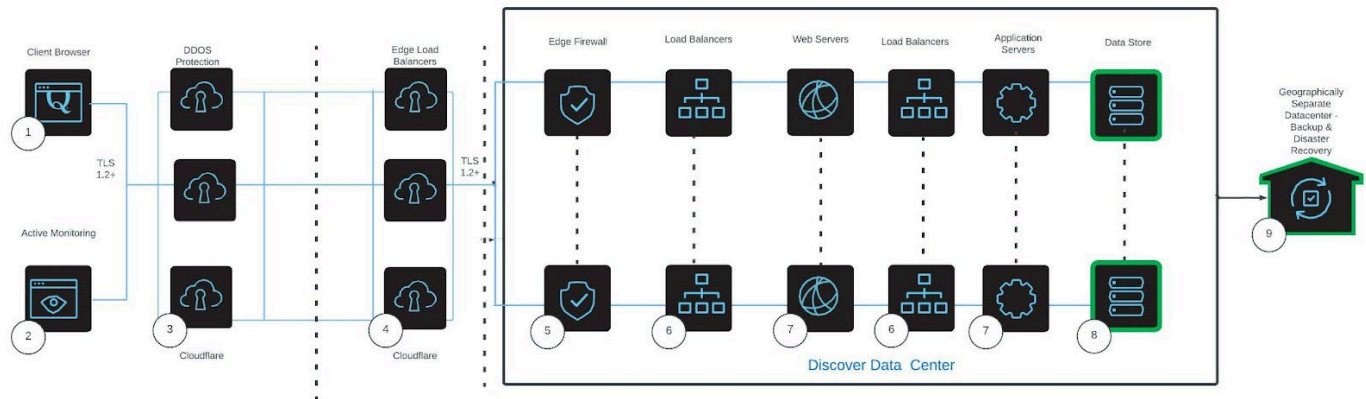
## ENCRYPTION KEY MANAGEMENT

Bring your own key (BYOK) is not supported.

## Password Policies for the service

- This section applies to password policies available within the platform and can be modified by the administrator to support the customer password policy. The default settings are as follows:
  - Minimum 10 characters; special character enabled.
  - Maximum age 90 days
  - Limit count of previous password reuse is 3
- Single Sign-On: Only SAMLv2 and OAuth integration are supported.

## DATA FLOW



1. **Client Browser** - Clients can access XM Discover or Qualtrics Social Connect from modern browsers without the need for any plugins or other software. Connections are over TLS v1.2 (or greater) with HSTS.
2. **Active Monitoring** - External monitoring service continually measures availability and performance (including page load times) from multiple locations globally
3. **DDOS Protection** - Security, Geo-blocking and DDoS protection delivered via Cloudflare web application firewall (WAF).
4. **Edge Load Balancers** – Edge load balancers are used to distribute load across the edge firewalls to improve reliability, resilience, and performance.
5. **Edge Firewall** - All direct access to XM Discover or Qualtrics Social Connect data centers are further protected via internal hardware firewalls.
6. **Load Balancers** - Load balancers distribute load across web and application servers to improve reliability, resilience, and performance.
7. **Web and Application Servers** – Web and application servers can be quickly scaled to accommodate demand for XM Discover or Qualtrics Social Connect services.
8. **Data Store** - Databases designed for scale and performance for both data collection and reporting. Data stores and responses are encrypted using AES-256 with XM Discover or Qualtrics Social Connect managed keys.
9. **Geographically Separate Datacenter - Backup & Disaster Recovery** - All data is backed up in a geographically separate data center (IBM or AWS) from production, in an encrypted format.

## XM DISCOVER USERS' PROFILE

Adding users to the platform requires defining their overall access and permissions by adjusting the following:

1. License
2. Permissions
3. Data Access (for linked users only).

1. **LICENSE:** A license defines the range of permissions that may be granted to a user and whether a user can be linked to a content provider. The four different user license types offer varying degrees of access to the product suite.

- **Configuration Analyst:** A person that has access to tune enrichments and manage connectors.
- **Activation Lead:** person that has configuration analyst permissions and also monitors user performance. This person is also able to manage cases.
- **Report Creator:** A person that can create dashboards.
- **Report Consumer:** A person that can view dashboards, initiate cases, and access reports on mobile.

2. **PERMISSIONS:** Permissions define the actions a user is allowed to perform in Studio. A user's license defines the maximum set of permissions a user can be granted. There are two sources of permissions for a user: individual permissions and group permissions, which are combined into user's derived permissions.

3. **DATA ACCESS:** Data access defines account and project level permissions for linked users in Designer. It is only required if you need to create report widgets in studio.

- Where does data come from? Studio gets data from a Content Provider, a Designer instance that contains customer feedback with sentiment, classification, and other enrichment data.
- User linking to use data in Studio widget, a user must be linked to a corresponding content provider and have appropriate level of data access to the designer project holding the data. Once these widgets are configured by the dashboard owner, they can be shared with any Studio user (dashboard viewer) regardless of the receiver's access level.

## QUALTRICS SOCIAL CONNECT PROFILES

By default, Social Connect offers five user roles. For each user a Customer adds to its account, the Customer can choose one of these user roles: Viewer, Contributor, Editor, Manager and Administrator.

- A **Viewer** is a user who has read-only access in Social Connect.
- A **Contributor** is a user who has more permissions than a viewer. They can assign mentions to team members, add tags to mentions, create drafts for new messages etc.
- An **Editor** is a user who has more permissions than a contributor. Most importantly, these users have the permission to post new messages / reply with the social profiles linked to Social Connect.
- A **Manager** is a user who has nearly all permissions. He or she is even able to update the account settings. In other words, this user can create, update, and delete topics.
- An **Administrator** is a user who has all permissions. The administrators are the only users able to add, edit and delete users to / from the account.

Custom user role creation is also available as an enhanced feature.

**Security Certifications:** The ISO 27001, 27017, 27018, and 27701 security certifications apply to XM Discover and Qualtrics Social Connect platforms. XM Discover and Qualtrics Social Connect (US Only) are also HITRUST certified.



**27001**

ISO 27001

Security Management Controls



HITRUST

CSF v9.2



**27701**

ISO 27701

Data Privacy Controls



**27017**

ISO 27017

Information Technology Security  
Techniques



**27018**

ISO 27018

Information Technology  
Security Techniques

## Appendix G: Additional Security and Privacy Framework for XM Journeys

XM Journeys offerings follow the same or similar practices and principles as stated above with the following exceptions.

### **Locations and Infrastructure**

XM Journeys is hosted by third-party data centers that are audited using industry best practices. The infrastructures are hosted in Amazon Web Services. These production data centers are located in the following regions:

- United States (Oregon)

### **Business Continuity & Disaster Recovery**

XM Journeys performs an annual disaster recovery test.

### **Backup Management**

XM Journeys maintains backups for up to 35 days.

### **Data Management**

XM Journeys is not compatible with Data Isolation. BYOK is also not supported. Data deletion and data exportation require the assistance of customer support.

### **Identity and Access Management**

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

- Passwords must be a minimum password complexity of 8 characters and must contain a combination of letters, numbers, and symbols based on available system functionality
- Password maximum lifetime is restricted to 90 days
- Passwords cannot be reused for at least 3 generations

XM Journeys does not require MFA to access their VPN.

### **Systems Monitoring**

XM Journeys maintains logs for up to 90 days.