alteryx

# INFORMATION SECURITY PROGRAM DESCRIPTION

Alteryx maintains an information security program (the "Program") that utilizes policies, standards, and procedures to protect the confidentiality, integrity and availability of information and data, whether in electronic or tangible form.

The Program includes appropriate administrative, technical, and physical controls designed to safeguard Alteryx's networks, systems and data, including Customer Content, in accordance with relevant privacy, data and security regulations and laws ("Security Standards").

Capitalized terms used in this document are defined in Attachment 1.

## 1. Organizational Security Standards

1.1. **Program Framework**. The Program is based on ISO/IEC 27001:2013 and is designed to:

a. prevent unauthorized access, acquisition, release, modification, or use of Customer Content; and

b. protect against threats or hazards to the security or integrity of Customer Content based on a current understanding of the security environment and evolving risk factors.

Alteryx implements and maintains information security measures in accordance with Alteryx's policies and standards, which may change from time to time in Alteryx's sole discretion, but which shall be no less stringent than the information security requirements outlined in this document.

1.2. **Certifications and Audits**. Alteryx will make available to its customers, upon reasonable written request, evidence of any third-party audits or certifications it maintains in the ordinary course of business, such as SSAE 16 – SOC1, SOC2, SOC3 attestations and ISO/IEC 27001 certifications, as applicable.

1.3. **Data Neutrality**. Except to the limited extent set forth in Section 2.3, Alteryx personnel do not interact with Customer Content in the normal course of business and Alteryx cannot determine the types and nature of data used as Customer Content. Customer is solely responsible for compliance with any laws and regulations and industry or professional standards specific to the Customer and its Customer Content. Alteryx does not represent or warrant that the Services or the Program meet a customer's regulatory and compliance requirements (such as PCI or ePHI requirements).

1.4. **Subprocessor Assessments**. Prior to engaging a new third-party service provider that will process Customer Content, Alteryx will conduct a risk assessment of the Subprocessor's data security practices, as well as conduct periodic reviews to assess whether their data security practices continue to meet Alteryx's information security obligations. Alteryx contractually binds all Subprocessors to minimum confidentiality, privacy, and security practices in line with Alteryx's obligations to customers and regulatory compliance.

## 2. Our People Standards

2.1. **Security Ownership**. Alteryx has appointed one or more dedicated information security officers responsible for coordinating and monitoring the Program. Officers appointed to these roles have the knowledge, experience, and authority to serve in this capacity.

2.2. **Security Roles and Responsibilities**. Alteryx allocates security responsibilities in accordance with its approved information security policies, which are communicated to employees and relevant third parties required to comply with such policies. Alteryx also integrates information security into its project management processes to identify and appropriately address information security risks.

2.3. **No Interaction with Customer Content**. Alteryx personnel do not directly interact with Customer Content except when a support request is initiated by a customer and access is for a limited term and purpose, as agreed with customer in advance or for limited security and administration purposes. All such access is monitored and logged to validate compliance with Alteryx security policies and procedures. Only those security and support personnel with a need-to-know are provided access to Customer Content and only after completing mandatory training and attesting to strict confidentiality for all such information.

2.4. **Confidentiality and Security Obligations**. All Alteryx personnel are engaged subject to confidentiality obligations. Employees acknowledge receipt and understanding of Alteryx's policies governing security, including our Code of Ethics and Acceptable Use Policy, during onboarding and annually thereafter.

2.5. **Security Training**. Alteryx requires annual security and privacy training for all personnel. General security awareness information is regularly made available to all personnel to reinforce their training. Additional, role-specific training, such as secure coding and OWASP (Open Web Application Security Project) for engineers, is provided periodically. Personnel are made aware of the possible consequences of violating Alteryx's security policies and procedures, which may include termination of employment or engagement with Alteryx.

2.6. **Personnel Background Checks**. To the extent permitted by law, Alteryx performs appropriate background checks on all personnel who have access to Alteryx networks, systems, and confidential data.

## 3. Physical Security Standards

3.1. **Facility Security**. Alteryx systems and information assets are physically protected to reduce the possibility of accidental or deliberate tampering or destruction as well as against theft or compromise.

3.2. **Employee Badging**. Alteryx personnel are provided with access and photo ID badges that are required to enter Alteryx offices and must be worn at all times. Employees are encouraged to challenge unknown individuals not properly displaying badge identification. Badge access is deactivated upon employee termination.

3.3. **Facility Access Controls**. Alteryx facilities are secured using RFID badge access to authorized areas, monitored entrances to prevent unauthorized access, and building CCTV. Visitor procedures require sign-in, issuance of a visitor badge and employee escorts while at the facility.

3.4. **Data Center Safeguards**. Alteryx-utilized data centers are required to have a physical security plan that includes entry protections, employee rules, environmental controls and safety equipment.

## 4. Technological and Operational Security Standards

4.1. **Network Security**. Alteryx maintains network devices and servers in data centers that employ industry standard security procedures and tools as described in this Section 4.

4.2. **Application Security**. Alteryx uses a risk-based approach when applying agile software development methodologies, which includes performing security architecture reviews, open-source library scans, ongoing and continuous monitoring, and external penetration testing in the development environment. Alteryx performs security code reviews and scans of application software it develops to detect malicious threats.

4.3. **Secure Coding Environments**. Alteryx logically or physically separates environments for development, testing, and production. Customer Content is not used in development or testing environments.

4.4. **Customer Content Hosting**. With respect to Services for which data hosting is managed by Alteryx, Customer Content is stored in secure, customer-specific environments. Users may delete the content they upload or link to the Services as part of the self-service options available within Alteryx products. Alteryx logically separates each customer's Customer Content from all other Alteryx and third-party data, including data of other Alteryx customers.

4.5. **Encryption**. Alteryx utilizes appropriate industry standard encryption technology, including encryption protocols, file encryption, and database encryption to protect Customer Content both in transit and at rest. Policies and standards are maintained to restrict access to cryptographic keys used for encryption of Customer Content. Customer Content hosted with third-party cloud providers is encrypted at rest using AES-256 or equivalent encryption. Data in transit is secured via HTTPS with TLSv1.2 or higher. SSL/TLS is supported for web browser clients and Alteryx corporate wireless networks use Advanced Encryption Standard (AES) with a minimum of Wi-Fi Protected Access 2 (WPA2). Alteryx employee laptops are secured with drive-level encryption.

4.6. **Access and Authentication**

a. **User Access Management**. Alteryx maintains access control policies and standards to support creation, modification, and deletion of Alteryx user accounts for systems or applications that store or allow access to Customer Content. Access is removed or restricted when no longer required or appropriate, and access is promptly removed following termination. Alteryx access practices include access control lists, role-based access controls and firewall rules.

b. **Least Privilege**. Personnel having access to Alteryx's networks, systems and confidential data have appropriately controlled and limited access. Alteryx's user account and access provisioning process assigns and revokes access rights to systems and applications, restricting access to only those Alteryx personnel and Subprocessors with a need-to-know and to the extent required to fulfill Alteryx's obligations or to comply with Applicable Law.

c. **Secure User Authentication**. Alteryx maintains authentication policies and standards for personnel with access to Alteryx networks and systems, including by assigning unique access credentials and prohibiting personnel from sharing Alteryx-assigned access credentials.

d. **Passwords and Multi-factor Authentication**. Alteryx maintains authentication policies and standards for all personnel accounts that have access to Alteryx networks and systems.

e. **Password Construction**. Where authentication is based on passwords, minimum password construction requirements include:

   i. Character length of at least eight characters for standard user accounts and enhanced minimum requirements for privileged accounts.

   ii. Complexity requirements including at least one lower case alpha, one upper case alpha, one number, and one special character.

   iii. Restrictions on word use (such as dictionary words) and prior password reuse.

f. **Password Maintenance**. Unsuccessful log-in attempts are strictly limited. Inactive accounts are periodically reviewed for deprovisioning. User passwords are generally subject to 90-day rotation requirements, except when Alteryx may permit other industry accepted requirements that are designed to provide equal or better security than standard password rotations.

g. **Multi-factor Authentication**. Alteryx has implemented and maintains multi-factor authentication ("MFA") for access to applications, systems, and confidential data.

4.7. **Virtual Private Networks**. Alteryx has implemented policies and standards requiring Alteryx personnel to use an Alteryx-provisioned Virtual Private Network ("VPN") when connecting to Alteryx's networks used to process Customer Content. Alteryx VPN connections require MFA and are encrypted using industry standard encryption.

4.8. **Malware Defenses**. Anti-malware software is deployed on Alteryx enterprise assets and endpoints and configured for automatic updates.

4.9. **Vulnerability and Patch Management**. Alteryx maintains a vulnerability management process to identify and remediate vulnerabilities by performing vulnerability scans, implementing vendor patches or fixes, and developing a patching timeline and remediation plan as appropriate based on the severity of the vulnerability. All identified systems are scanned for vulnerabilities on a weekly basis. Patch cadence is assigned based on Common Vulnerability Scoring System ("CVSS") scores (Critical, High, Medium, and Low). Alteryx applies security patches on a regular basis to systems used to access or process Customer Content.

4.10. **Intrusion Detection**. Alteryx has implemented intrusion detection systems at the network and/or host level to detect unwanted or hostile network traffic. Alteryx will update its intrusion detection software regularly, on a scheduled basis, following the availability of updates by the software provider.

4.11. **Incident Response Plan**. Alteryx maintains an incident response program that is derived from industry standards, including ISO/IEC 27035:2016 and NIST 800-61, to address Security Incidents and suspected unauthorized access to Alteryx systems that process or have access to Customer Content. The incident response program incorporates mechanisms designed to:

a. **Identify and Analyze**. Identify, analyze, and document relevant indicators of a Security Incident. Confirm the nature and extent of a Security Incident. Provide notification to relevant individuals, entities, or authorities in accordance with Alteryx's contractual and legal obligations.

b. **Containment, Eradication and Recovery**. Contain the impact or harm caused by a Security Incident and work to eliminate the Security Incident from impacted Alteryx networks and systems and return to normal operations. Gather and maintain evidence of the Security Incident.

c. **Learn**. Understand and learn from a Security Incident to determine whether to adopt any improvements to defenses, incident response or other procedures.

4.12. **Change Control**. Alteryx maintains policies and standards for managing changes and updates to production systems, applications, and databases designed to ensure security patching, authentication, and testing is performed prior to implementing changes in production.

4.13. **Security Logs**. Alteryx maintains logs of relevant security information gathered from systems and applications. These logs capture key security event types used to detect suspicious system or user behaviors. Security logs are retained for a minimum of 90 days.

4.14. **Testing and Audits**

a. **Penetration Tests**. At least once annually, Alteryx undertakes penetration testing of its products by an independent third party. Findings are remediated in a timeframe that is commensurate with any identified risks.

b. **Vulnerability Scanning**. Alteryx maintains a vulnerability management program and performs regular vulnerability scanning against services and key infrastructure utilizing industry standard tools or well-known external suppliers.

4.15. **Business Continuity and Disaster Recovery**. Alteryx maintains a business continuity and disaster recovery program ("BC/DR Program") aligned to ISO/IEC 22301 that provides ongoing performance and restoration of business functions and services following any significant disruption to operations. The BC/DR Plan includes:

a. back-up recovery processes designed so that critical business functions can be resumed within defined timeframes; and

b. a process to regularly review, test and update the BC/DR Program plans at least annually and when otherwise needed.

## Attachment 1 – Definitions

| Term | Definition |
|---|---|
| **Applicable Law** | The relevant data protection and data privacy laws, rules, and regulations directly applicable to the Program, including, but not limited to, the General Data Protection Regulation (EU 2016/679) ("**GDPR**") and the California Consumer Privacy Act and California Privacy Rights Act ("**CCPA/CPRA**"), the Virginia Consumer Data Protection Act ("**VCDPA"),** and any successor laws, rules and regulations. For the avoidance of doubt, "Applicable Laws" will include other state, federal, and international data protection and data privacy laws not expressly named above to the extent directly applicable to the Program, including any new laws, rules and regulations that take effect after the publication of this document (*e.g.,* the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Data Privacy Act). |
| **Customer Content** | Any data or information that a customer uploads, connects to, or imports into the Services, from its internal data sets or other sources not supplied by Alteryx (*i.e.,* Licensee-Sourced Data) to facilitate the customer's use of such Services, together with any workflows, recipes, insights, or other materials created by a customer using the Services, and any log-in credentials for accessing or linking to third-party data sources while using the Services. Customer Content includes logs uploaded by a customer related to a support request and any raw data provided or made accessible to Alteryx or its Subprocessors in providing professional services pursuant to an Alteryx Order Form. For the avoidance of doubt, Customer Content is considered "Licensee-Sourced Data" under the Alteryx End User License Agreement. Usage Data, as defined in the Alteryx Data Protection Agreement, is expressly excluded from Customer Content. |
| **Personal Data** | "Personal data", "personally identifiable information", or "personal information" are as defined under Applicable Law (collectively here, "Personal Data"). |
| **"process", "processes", "processing" and "processed"** | Any operation or set of operations which is performed on Personal Data or sets of Personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. |
| **Security Incident** | An unauthorized or unlawful breach of Alteryx security leading to the accidental or unauthorized destruction, loss, alteration, disclosure of, or access to Customer Content. |
| **Services** | All Alteryx cloud-based products, professional services, and support services provided to a customer pursuant to a fully executed Alteryx Order Form. |
| **Subprocessor** | Contractors, vendors and third-party service providers engaged by Alteryx to process Customer Content. |