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. **Scope.** The Program encompasses all systems for which Alteryx has administrative responsibility, including systems managed or hosted by third parties on behalf of Alteryx. It includes assets owned, leased, controlled, or used by Alteryx employees, its agents, temporary employees, contractors, or other business partners acting on behalf and as instructed by Alteryx ("Personnel").

1.2. **Program Framework**. The Program aligns to ISO/IEC 27001:2013 and is designed to:

a. prevent accidental or unauthorized destruction, loss, alteration, disclosure of, or access to Customer Content; and

b. protect against threats or hazards to the confidentiality, integrity and availability 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.

1.3. **Certifications, Attestations and Audits**. Alteryx will make available to its customers, upon reasonable written request and subject to appropriate confidentiality obligations, evidence of any third-party audits or certifications it maintains in the ordinary course of business, such as SOC 2 Type 2 assessments and ISO/IEC 27001 certifications/attestations, as applicable. Alteryx's ISO/IEC 27001 certification is also made available on Alteryx's Trust website located at www.alteryx.com/trust.

1.4. **Data Neutrality**. Except to the limited extent set forth in Section 2.4, Alteryx Personnel do not interact with Cloud Content in the normal course of business and Alteryx cannot determine the types and nature of data included by customers in Cloud Content. Customers are solely responsible for compliance with any laws and regulations and industry or professional standards specific to a customer and its Cloud 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).

1.5. **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.

1.6. **Data Classification**. Alteryx information assets, including digital, electronic, and physical information assets, are assigned a sensitivity level (a "Classification") based on regulatory, legal, contractual, potential impact of loss or other requirements as determined by Alteryx. Based on the applied Classification, appropriate data handling controls are implemented to protect the information assets against unauthorized use or disclosure.

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. **Separation of Duties**. Areas of responsibility are separated to reduce opportunities for unauthorized or unintentional modification or misuse of Alteryx assets. Personnel roles are defined in accordance with job descriptions to support the separation of duties across multiple users. Mission critical functions and system support functions have appropriate separation of duties and backup Personnel to help maintain continuity of operations.

2.4. **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 the 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.

2.5. **Confidentiality and Security Obligations**. All Personnel are expected to abide by Alteryx's information security policies and 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.

2.6. **Security Training**. Alteryx requires annual security and privacy training for all Personnel. General security awareness information is regularly made available to 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.

2.7. **Personnel Background Checks**. To the extent permitted by law, Alteryx requires 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 photo ID badges that are required to enter Alteryx offices and must be worn at all times. Employees are instructed to challenge unknown individuals not properly displaying badge identification. Badge access is promptly 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 maintain a documented 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. Alteryx has implemented and maintains application security policies and standards to support secure application coding practices, such as referencing OWASP's Application Security Verification Standard ("ASVS") and the Common Weakness Enumeration ("CWE") list for code verification and the Common Vulnerabilities and Exposures ("CVE") database to identify known Vulnerabilities. Alteryx application security testing processes include, as applicable, dynamic and static application security testing, software composition analysis and other industry standard application security testing methodologies.

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 secured 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. 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. Administrative and technical measures are implemented to protect cryptographic keys used to secure Customer Content against disclosure and misuse, including implementation of industry standard master key management practices, secure key storage practices, access restriction to keys limited to the fewest number of key custodians necessary, and enablement of appropriate audit and logging trails.

4.6. **Access and Authentication Policies and Standards**

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. User access reviews are performed at regular intervals for user, service and privileged accounts. Such reviews seek to identify and address anomalous access rights including accounts for terminated employees, inappropriate access rights, unauthorized elevated privileges, separation of duties issues, unauthorized generic or shared accounts, and developer access to production environments.

b. **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.

c. **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 Personnel and Subprocessors with a need-to-know and to the extent required to fulfill Alteryx's obligations or to comply with Applicable Law.

4.7. **Password Management and Multi-factor Authentication**

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

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

i. Character length of at least ten 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.

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

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

4.8. **Remote Access**

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

b. **Remote Assets**. Alteryx manages access control for assets remotely connecting to Alteryx resources. The amount of access granted for authorized remote assets is determined based on factors including compliance with Alteryx's secure configuration requirements and the presence of an up-to-date operating system, anti-malware and other application software.

4.9. **System Defense**

a. **Malware Defenses**. Malware defenses are implemented to detect and prevent the installation, spread and execution of malicious applications, code and scripts on enterprise assets. Anti-malware software is deployed on Alteryx enterprise assets and endpoints and configured for automatic updates.

b. **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.

c. **Incident Response Plan**. Alteryx maintains an incident response plan 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:

i. **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.

ii. **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.

iii. **Learn**. Following the resolution of a Security Incident, Alteryx will conduct a post-incident review. This review will include an analysis of the Security Incident, its impact, the effectiveness of the incident response, and any

necessary changes to the existing policies or procedures based on the lessons learned.

4.10. **System Maintenance and Updates**

a. **Vulnerability and Patch Management**. Alteryx maintains a Vulnerability management process designed to promptly identify and remediate Vulnerabilities in Alteryx's network, systems, Products and Services. Alteryx monitors public and private industry sources for new threats and Vulnerabilities and regularly scans for Vulnerabilities using industry standard tools and methodologies. Once a Vulnerability is identified, Alteryx promptly assesses the risk of the Vulnerability, and prioritizes and implements a remediation response appropriate for the associated risk. Alteryx monitors the implemented remediation response to verify its effectiveness and may take additional measures as necessary.

i. **Network and Systems**. Alteryx automatically updates application and operating systems using vendor-supplied security patches on a quarterly basis or earlier when needed.

ii. **Software Patching**. Alteryx assigns a Vulnerability patching cadence for Products and Services based on the Common Vulnerability Scoring System ("CVSS") using CVSS Base, Temporal and Environmental metrics ("CVSS Scores") and grouped into Critical, High, Medium, and Low Vulnerabilities. Patches are prioritized according to CVSS Scores and deployed in scheduled Product releases or Service updates, except in circumstances when Alteryx determines, based on CVSS temporal and environmental factors (such as Exploit Code Maturity, Remediation Level, Report Confidence and Security Requirement Metrics), there is a more immediate potential for exploitability, in which case patches are prioritized for earlier release. Alteryx follows responsible and coordinated Vulnerability disclosure practices that balances the need for public awareness with the risk of exploitation.

b. **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.

4.11. **Security Logs**. Alteryx maintains centralized and time synchronized audit 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. System administrator and system operator activities are also logged and reviewed at appropriate intervals. Security logs are retained for a minimum of 90 days.

4.12. **Testing and Recovery**

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 performs regular vulnerability scanning against services and key infrastructure utilizing industry standard tools and services.

c. **Data Recovery**. Alteryx has implemented data recovery practices designed to recover data in the event of an incident or similar occurrence. Full and incremental backups on enterprise assets are regularly performed and data restoration procedures are documented. Backup restoration and integrity testing is periodically performed.

d. **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:

   i. business impact analysis to help Alteryx business units prioritize functions necessary to continue operations during and after a disruption;

   ii. business continuity plans to document appropriate responses to scenarios related to loss of Personnel, work areas, applications, vendors, upstream departments and resources;

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

   iv. a process to regularly review, test and update the BC/DR Program plans at least annually and when otherwise needed. Failover tests, table-top exercises and drills are included in the testing methodology. Alteryx engages third-party evaluators to attest annually to the efficacy of the BC/DR Program.

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).
Cloud Content	Any data or information that a customer uploads, connects to, or imports into Alteryx cloud environments for use with the Services, from its internal data sets or other sources not supplied by Alteryx (*e.g.,* Licensee-Sourced Data), together with any workflows, recipes, insights, or other materials created by customer using the Services, and any log-in credentials for accessing or linking to third-party data sources while using the Services.
Customer Content	Collectively, Cloud Content and Services 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.
Products	For purposes of this Information Security Program Description, Alteryx on-premises software purchased by Customer, together with the applicable updates to such Products as provided by Alteryx. Products do not include Products that Alteryx has designated as end-of-life.
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.
Services Content	Services Content includes logs uploaded by the 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 Order Form.
Subprocessor	Contractors, vendors and third-party service providers engaged by Alteryx to process Customer Content.
Vulnerability	Has the meaning set forth in NIST 800-30, which defines a "vulnerability" as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.