ALTERYX SECURITY STANDARDS

Alteryx abides by the security standards set out herein. Alteryx may update or modify these security standards from time to time, in its sole discretion, provided that such modifications will not result in a material degradation of the security of the relevant Licensed Products and any services (collectively, the "**Services**") during the term of the Agreement.

1. GENERAL PROVISIONS

1.1 Data Neutral. Alteryx is unaware of which data types its customers upload to and use with the Services and will process all data, regardless of its nature, as long as it fits the pre-defined characteristics that allow it to be processed as part of the Services.

1.2 No Employee Interaction. Alteryx employees do not directly interact with Licensee Content as part of their normal job duties except for the purpose of providing support services to customers upon request and as agreed in advance.

1.3 Licensee Content. Licensee Content is preserved in encrypted form using industry standard encryption, in customer-specific S3 buckets. Each Authorized User may delete the content they upload or link to the Services as part of the self-service options available within the Alteryx platform.

1.4 Shared Responsibility. Alteryx customers are strongly discouraged from sending highly sensitive data (such as PCI or ePHI) to the Services. Alteryx provides appropriate security for its Services but each customer must take care to use all Services responsibly and in accordance with any industry or professional standards applicable to such customer. Licensee must also maintain appropriate controls to secure Licensee's user accounts and credentials.

1.5 Industry Requirements. Licensee is responsible for understanding and applying any laws, regulations, or industry standards specific to Licensee's industry or Licensee Content.

1.6 Definitions:

1.6.1 Licensee – the entity that licenses relevant Alteryx Licensed Products pursuant to the Agreement

1.6.2 Licensee Content – Licensee's intellectual property, confidential information, and any Personal Data processed for or on behalf of the Licensee as part of the information uploaded or connected to the relevant Licensed Products by Licensee for Licensee's exclusive use

1.6.3 Personal Data – as defined by the DPA

1.6.4 Subprocessor- as defined by the DPA

2. INFORMATION SECURITY PROGRAM

2.1 Information Security Program. Alteryx maintains an information security program (the "**Program**") that utilizes policies, procedures, and standards to protect the confidentiality, integrity and availability of information and data, whether in electronic or tangible form. The Program is based on ISO/IEC 27001 and (i) defines, implements and includes periodic reviews of Alteryx's information security policies and procedures, including those for accessing and transmitting Licensee Content; (ii) is designed to prevent unauthorized access, acquisition, release, modification or use of Licensee Content; and (iii) is designed to protect against threats or hazards to the security or integrity of Licensee Content based on a current understanding of the security environment and evolving risk factors.

2.2 Control Requirements. Alteryx maintains adequate administrative, technical, and physical controls designed to safeguard Licensee Content in accordance with relevant privacy, data, and security regulations and laws ("**Security Standards**"). Alteryx's Security Standards consider the sensitivity of the Services and the risks that pertain to processing of Licensee Content as part of the Services and as contemplated by the Agreement.

2.2.1 User Access Management. Alteryx implements access control policies to support creation, amendment, and deletion of user accounts for systems or applications storing or allowing access to Licensee Content. 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 that require access, and solely to the extent so required, to fulfill Alteryx's obligations under the Agreement or to comply with applicable law.

2.2.2 Secure User Authentication. Alteryx ensures proper user authentication for all of its personnel with access to Licensee Content, including by: assigning each employee unique access credentials for the system on which Licensee Content may be accessed and prohibiting employees from sharing their access credentials; and using access control lists and firewall rules. Alteryx ensures that all persons having access to Alteryx systems or any Licensee Content have appropriately controlled and limited access, access is removed or restricted when no longer required or appropriate, and access is promptly removed following termination.

2.2.3 Personnel Training and Background Checks. Alteryx provides annual security awareness and privacy training to all personnel who process or may have access to Licensee Content. Where permitted by law, Alteryx performs adequate background checks on all personnel who have access to Licensee Content.

2.2.4 Passwords and Multi-factor Authentication. Alteryx maintains industry standard password security for all employee accounts. Policies include minimum length, complexity, restrictions on password reuse, number of password resets in a given timeframe, and frequency in which passwords must be changed. Alteryx has implemented and maintains a multi-factor authentication method required for access to applications and systems containing or accessing Licensee Content.

2.2.5 Subprocessor Assessments. Prior to engaging new third-party Subprocessors that will have access to Licensee Content, Alteryx will conduct a risk assessment of the data security practices of such Subprocessors, as well as periodic reviews to ensure their data security practices continue to meet Alteryx's obligations hereunder and, where applicable, the DPA.

2.3 Data Security

2.3.1 Encryption. Alteryx utilizes current encryption technology, including encryption protocols, file encryption and database encryption, to protect Licensee Content both in transit and at rest.

2.3.2 Vulnerability & Patch Management. Alteryx maintains a vulnerability management process to identity and remediate vulnerabilities by performing vulnerability scans, implementing vendor patches or fixes, and developing a remediation plan for critical vulnerabilities. Alteryx applies security patches on a regular basis to systems used to access or process Licensee Content.

2.3.3 Data Separation. Alteryx logically separates Licensee Content from all other Alteryx and third party data.

2.3.4 Incident Response Plan. Alteryx maintains an incident response program to address any suspected unauthorized access to or use of Licensee Content or to Alteryx systems that process or have access to Licensee Content, including, but not limited to: (i) promptly notifying Licensee of a confirmed breach, together with sufficient detail to inform Licensee of any potential risks to Licensee systems or data; (ii) taking all reasonable steps required to address the source of the suspected breach and to mitigate any identified risks; and (iii) providing Licensee with updates and information to demonstrate adequate resolution of the vulnerabilities giving rise to the suspected breach.

2.3.5 Policies. Alteryx maintains policies and procedures to prevent the unauthorized disclosure or use of Licensee Content and ensures that Alteryx personnel attest to such policies and procedures upon hire and annually thereafter.

2.3.6 Alteryx limits access to Alteryx computers and networks that process or may access Licensee Content through the use of one or more of the following: (i) username & password; (ii) multi-factor authentication; (iii) access control lists; and (iv) firewall rules.

2.3.7 Alteryx maintains network devices and servers in data centers that employ industry-accepted procedures and tools, including, at a minimum: (i) restricting both physical and network access to those with a business need for access; (ii) restricting physical access to the data centers by card-key control systems; (iii) implementing a network-based intrusion detection and prevention system; (iv) implementing firewalls to segment networks; (v) implementing security vulnerability assessment processes and tools; (vi) implementing change management procedures; (vii) implementing patch management processes and tools; and (viii) periodically backing up data maintained on Alteryx network servers and encrypting back-up media for storage off-site.

2.4 Application Security

2.4.1 Change Control. Alteryx maintains policies and procedures for managing changes and updates to production systems, applications, and databases, including processes for documenting security patching, authentication, and the testing and approval of changes into production.

2.4.2 Key Management. Alteryx implements key management procedures that include the secure generation, distribution, activation, storage, recovery, and replacement of cryptographic keys. Keys are rotated on a regular basis and lost, corrupted, or expired keys are immediately revoked or disabled.

2.4.3 Logging**.** Alteryx logs security information from systems and applications that store, allow access to, or process Licensee Content. These logs capture key security event types upon the detection of suspicious system and/or user behaviors.

2.4.4 Intrusion Detection. Alteryx has implemented and maintains an intrusion detection monitoring process 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 such updates by the software provider.

2.4.5 Secure Coding Practices. Alteryx logically or physically separates environments for development, testing, and production. Licensee Content is not used in development or testing environments.

3. TESTING AND AUDITS

3.1 Penetration Tests. At least once annually, Alteryx undertakes penetration testing of the Licensed Products by an independent third party and promptly remediates all critical and high vulnerabilities identified in penetration test results. All other findings are remediated in a timeframe that is commensurate with the identified risks.

3.2 Compliance. Alteryx shall either provide attestation statements and reports regarding its security certification programs (where applicable) or complete Licensee's security questionnaire, upon Licensee's reasonable, written request. Requests for reports or security questionnaires are permitted once per rolling calendar year, provided, however, that Licensee may request additional assurances in the event of a confirmed breach of Alteryx's systems used to process Licensee Content.

3.3 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. DATA USE, RETENTION AND DELETION

4.1 Permitted Use. Alteryx may only use Licensee Content as outlined by and for the duration of the Agreement. Licensee Content may not be shared with third parties except as permitted by the Agreement, including, where applicable, the terms of the DPA. Notwithstanding an obligation of Alteryx to retain certain, limited Licensee Content for the period designated by applicable law or regulation, Alteryx may only retain Licensee Content as expressly permitted by Licensee for the purpose of providing the Services.

4.2 Secure Deletion. Upon expiration or termination of the Agreement for any reason, Alteryx shall promptly delete or destroy all Licensee Content, taking into account currently available technology so that Licensee Content cannot be reasonably read or reconstructed, including by rendering unreadable any media on which Licensee Content is stored.

4.3 Data Storage. Unless otherwise expressly agreed in an Order Form, Alteryx stores Licensee Content in the United States and may process License Content in order to provide the Services in any country in which Alteryx operates.

5. DISASTER RECOVERY & BUSINESS CONTINUITY

5.1 Alteryx maintains a disaster recovery/business continuity program that includes: (i) disaster recovery/business continuity plans and procedures; (ii) back-up recovery processes designed to ensure that critical business functions can be resumed within specified timeframes; and (iii) a process to regularly review, test and update the disaster recovery/business continuity program as needed.