TIBCO Security Policies, Practices and Processes

1. Security Policy. TIBCO maintains a company-wide information security management system and control program that includes security policies, standards and procedures based upon ISO/IEC 27001:2013. The TIBCO Security Policy:

   a. Requires the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of confidential information belonging to TIBCO’s customers to the extent that such information is provided to TIBCO and maintained or processed by TIBCO during its provision of Services (“Protected Data”);

   b. Evaluating and improving, where necessary, the effectiveness of TIBCO’s current safeguards to limit risks concerning Protected Data, including but not limited to:

      • Secure software development practices;

      • Secure operating procedures and vulnerability management

      • Ongoing employee training;

      • Means for detecting and preventing intrusions and security system failures on critical systems; and

   c. Ensures that only active TIBCO employees and contractors may access records containing Protected Data and limits access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with governmental record retention regulations;

   d. Ensures that Protected Data that is identified as such to TIBCO by the customer at intake, is compartmentalized and is handled in a secure environment, including any individual personal data provided to TIBCO by Customer as set forth in this Exhibit, using commercially available and industry accepted controls and precautionary measures;

   e. Ensures that commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;

   f. Requires monitoring of operations and maintaining procedures to ensure that Security Policies are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Protected Data, and upgrading information safeguards as necessary to limit risks;

   g. Mandates a security patch and vulnerability management process based on accepted industry practices standards and protocols, including secure development and security training for all developers, monitoring threats, and responding to vulnerabilities reported by third parties; and

   h. Provides security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Protected Data.


   a. Customer will notify TIBCO before providing or transmitting any Protected Data to TIBCO during TIBCO’s Services. In the event that TIBCO agrees to receive Protected Data from Customer, TIBCO will manage and/or process such Protected Data pursuant to the security requirements, obligations, specifications and event reporting procedures as set forth in this Exhibit and the Agreement, and any amendments.

   b. TIBCO will comply with: (i) secure software development practices consistent with industry accepted standards and practices,
and (ii) industry best practices on privacy and security.

3. Patch and Vulnerability Management

a. TIBCO follows commercially reasonable best practices for patch management, criticality ranking and patching time frame requirements for all IT systems, switches, routers, appliances, servers, and workstation PC’s.

b. TIBCO ensures that trusted, commercially available anti-virus software is installed, enabled, and kept current on TIBCO servers and systems used in accessing, processing, transmitting, or storing Protected Data.

c. TIBCO maintains trusted, current, commercially available spyware protection on TIBCO PC’s, particularly those used for accessing, processing, transmitting, or storing Protected Data.

d. TIBCO maintains a vulnerability management solution for devices connected to TIBCO’s LAN. Such solution is designed to regularly scan TIBCO’s network for known vulnerabilities


a. TIBCO regularly monitors the key controls of critical systems, network and procedures of TIBCO’s Security Guidelines to validate proper implementation and effectiveness in addressing the threats, vulnerabilities and risks identified. This monitoring is variable by the criticality, exposure, and the systems assets and may include: (i) internal risk assessments; (ii) validation of Multi-Factor Authentication for select environments; (iii) third party compliance, including hosting services and third party components; and (iv) assessing changes affecting systems processing authentications, authorizations, and auditing.

b. TIBCO performs periodic vulnerability assessments on TIBCO’s critical applications and systems. Penetration tests are performed either by TIBCO or by an established, reputable independent third party.


a. TIBCO performs periodic risk assessments that evaluate and assess the security of the system's physical configuration and environment, software, information handling processes, and user practices including appropriate logs and reports on security activity.

b. In addition, Security Policies are regularly reviewed and evaluated to ensure operational effectiveness, compliance with applicable laws and regulations, and to address new threats and risks.

c. Security Policies are also reviewed when there is a material change in TIBCO's business practices or the external threat environment that may reasonably implicate the security or integrity of records containing Protected Data. TIBCO uses a documented change control process for software, systems, applications, and databases that ensures access changes are controlled, approved, and recorded.
d. TIBCO will promptly notify Customer of any planned system configuration changes or other changes that would adversely affect the confidentiality, integrity, or availability of Customer’s Protected Data.


a. All developers of systems and software being delivered to Customer receive industry standard training in secure software development practices. Upon request, TIBCO will make available evidence of such qualifications, subject to any restrictions on the release of personal information pertaining to individual employees. For special classes of Protected Data, such as electronic Personal Health Information (ePHI) or sensitive personal data, TIBCO implements special compartmentalized data handling and those administrative, physical and technical safeguards required by applicable regulations such as those issued under the Health Insurance Portability and Accountability Act (HIPAA). TIBCO monitors, evaluates, and adjusts, as appropriate, the security guidelines in light of any relevant changes in technology and/or security and data privacy laws and regulations applicable to TIBCO. TIBCO takes reasonable measures to ensure that any third party service TIBCO uses has the capacity to protect Protected Data and apply proper safeguards to such Protected Data.

b. All agreements with third parties involving access to TIBCO’s systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), must specifically address security risks, controls, and procedures for information systems and contain terms, conditions and restrictions at least as protective and as restrictive as those set forth herein. TIBCO shall supply each of its personnel and contractors with appropriate, ongoing training regarding information security procedures, risks, and threats and TIBCO shall be responsible for the performance of any subcontractor. TIBCO has an established set of procedures to ensure personnel and contractors promptly report actual and/or suspected breaches of security. TIBCO agrees that any Services performed for Customer involving use of Protected Data shall be performed only at location(s) and by personnel permitted under the Agreement.

7. Secure Data Transmission. Any Customer Protected Data that TIBCO transmits over a public communications network will be protected during transmission using industry accepted standards, including encryption and VPNs.

8. Backup and Retention. TIBCO will regularly backup systems used to provide services to Customer to ensure adequate recovery capabilities. Back-ups will be appropriately protected to ensure only authorized individuals are able to access the Protected Data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records. If not separately backed up, TIBCO will secure any files containing Protected Data against unauthorized access in accordance with the terms of the Agreement until the backup tapes are recycled or properly destroyed so that information on them cannot practically be read or reconstructed.

9. Data and Media Disposal. TIBCO maintains procedures in conformance with the NIST SP 800-88 standard, regarding the disposal of both tangible property and electronic files containing Protected Data, taking into account available technology so that Protected Data cannot be reconstructed and read.

10. PII / PHI / Personal Data.

a. TIBCO will ensure compliance with applicable laws and regulations concerning the confidentiality, security and processing of any Protected Data that it receives from Customer, including, but not limited to the General Data Protection Regulation 2016/679 ("GDPR"), the EU Standard Contractual Clauses, Privacy Shield, the Health Insurance Portability and Accountability Act, and the California Consumer Privacy Act of 2018 ("CCPA"). In the event TIBCO processes types of Protected Data that are subject to additional regulatory requirements due to the nature of the data or its place of origin, TIBCO will reasonably cooperate with Customer to arrange compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law, implementation of additional security controls required by applicable law, completion of regulatory filings applicable to TIBCO, participation in regulatory audits, and responding to requests from data subjects to update or delete Protected Data.

b. In furtherance of the obligations stated herein, specifically with respect to the CCPA, TIBCO shall not retain, use, or disclose the Protected Data (i) except on behalf of Customer and pursuant to business purpose of performing the services stated in the Agreement and (ii) outside of the direct business relationship between TIBCO and Customer. Further, TIBCO shall not sell Protected Data that
Licenser Processes under the Agreement for any reason. TIBCO certifies that it understands and will comply with the restrictions stated in this subsection (b).

c. Customer agrees to the terms of TIBCO’s Privacy Policy found at https://www.tibco.com/company/privacy which are incorporated by reference.

11. Security Incident Management and Remediation. For purposes of this Exhibit, a “Security Incident” means any known or suspected impairment to the security of Protected Data, including any (i) act or omission that violates any law, industry requirement or any TIBCO security policy concerning Protected Data; or (ii) unauthorized access to or disclosure or acquisition of Customer’s Protected Data.

   a. TIBCO maintains a response function capable of identifying and assessing the seriousness and extent of a Security Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing and documenting remedial action plans, and preventing the recurrence of Security Incidents.

   b. Security Incidents on TIBCO’s systems are logged and reviewed quarterly, secured, and maintained for a minimum of twelve (12) months.

   c. TIBCO keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

   d. TIBCO will promptly notify the designated Customer security contact of any Security Incidents that compromise Customer’s Protected Data. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including the type of Protected Data that was the subject of the Security Incident and a description of measures being taken to address the occurrence, and any other information Customer reasonably requests. TIBCO will provide this information to Customer as soon as such information can be collected or otherwise becomes available.

   e. Following this initial notification, TIBCO will promptly investigate any Security Incident affecting Customer’s Protected Data and take all reasonable and necessary steps to prevent any further compromise of the Protected Data. If a security deficiency is identified within any TIBCO information system during this investigation, TIBCO will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Protected Data that was disclosed, destroyed, altered or compromised, and any investigative, corrective, or remedial actions taken or planned by TIBCO to mitigate the risk of further Security Incidents. TIBCO will maintain log files sufficient to enable Customer to determine what Protected Data was accessed and when, regardless of whether such data is physically or electronically maintained.

12. Business Continuity and Disaster Recovery. TIBCO maintains business continuity and disaster recovery planning to provide procedures for the continuity, recovery and operation of information systems and facilities that could impact Protected Data or any application or system directly associated with the accessing, processing, storage, communication or transmission of Protected Data (“DR Plan”). The TIBCO DR Plan includes procedures for responding to emergencies (e.g. natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes: (i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the Contingency and Disaster Recovery Guide including documenting the tests in writing.

13. Certifications. As pertains to the offering, TIBCO maintains multiple security certifications, including PCI-DSS, HITRUST, FedRAMP, SSAE-16 (SOC 1 and SOC 2), and ISO 27001. Certifications are obtained for particular areas or aspects of TIBCO’s information technology processes and procedures and may not apply on a company-wide basis.

14. Access and Review. TIBCO will make its security policies, procedures, and other security-related information related to Customer’s Protected Data available for Customer’s review at TIBCO upon reasonable prior written notice by Customer and subject to TIBCO’s confidentiality and security conditions, and subject to a written and mutually agreed audit plan. TIBCO reserves the right to require its prior approval to any third party review of the DR Plan, and reasonably condition and restrict such third party access.