TIBCO Information Security and Compliance Program
Last Updated: October 15, 2020
(Capitalized terms used below and not otherwise defined, are defined at https://terms.tibco.com/#definitions.)

1. **Information Security and Compliance at TIBCO.** This information security and compliance program states the data protection and cybersecurity measures that TIBCO Software Inc. and its Affiliates (collectively "TIBCO") implement, support, and maintain in order to: (1) protect Customer Protected Data; (2) develop and deliver safe and secure Software and services; (3) train Personnel on information security and compliance obligations; and (4) ensure continued business operations and access to services (the "Security Program").

   a. As documented herein, and in TIBCO's internal information security policies, TIBCO:

      i. implements and maintains industry standard physical, administrative, and technological measures to protect (1) Customer's Protected Data that TIBCO processes in connection with a Cloud Service, Maintenance, or Consulting Services from security incidents, (2) TIBCO's and its Customer's computing systems from unauthorized access or use, and (3) Software from vulnerabilities;
      ii. continually reviews and revises its measures to address new or ongoing risks to conform with industry best practices and legal requirements regarding software development, cybersecurity and privacy;
      iii. cooperates with Customers to (1) mitigate risks and reduce the impact of any unauthorized access to Customer's computing systems or disclosure, or (2) unauthorized use of Protected Data; and
      iv. requires Personnel to receive training on information security requirements and, with respect to subcontractors, maintain substantially similar, but no less protective, security practices and procedures to protect data and systems.

2. **General Requirements**

   a. Certifications. TIBCO's Security Program is based on internal policies regarding information security, data handling, and secure development practices, which are derived from applicable laws, regulations, and accepted industry standards, including ISO/IEC 27001/2, ISAE 3402/SSAE 18, the NIST Cybersecurity Framework, and PCI DSS. Certain products and processes are certified according to PCI-DSS, HITRUST, FedRAMP, SSAE-18 (SOC 2), and ISO 27001 standards. Upon a written request from Customer and to the extent available according to confidentiality requirements, TIBCO will provide a copy of the appropriate and available policies, reports, or certifications indicating compliance with the aforementioned standards.

   b. Security Group. TIBCO's information security team (the "Security Group") maintains this Security Program, which is reviewed for effectiveness at regular intervals. The Security Group also monitors TIBCO's operating procedures to ensure that TIBCO's processes are functioning as designed to prevent unauthorized access to TIBCO's and its Customer's systems, databases, and Protected Data. If submitted as part of a support request, TIBCO will provide the name and contact information of its designated information security representatives.

   c. Security Evaluations.

      i. TIBCO periodically reviews, evaluates, and assesses the security of TIBCO's physical premises, computing environment, Software, information handling processes, and user practices.
      ii. TIBCO reviews this Security Program regularly (or as required by applicable law) to ensure (1) operational effectiveness, (2) compliance with applicable laws and regulations, and (3) new threats and risks are addressed. The Security Program is also reviewed whenever there is a material change in TIBCO's business practices or when there is an external threat that may reasonably implicate the security or integrity of records containing Protected Data or Software delivered by TIBCO.
      iii. TIBCO uses a documented change control process for Software, systems, applications, and databases that process Protected Data to ensure access changes are controlled, approved, and recorded to avoid negative impacts to performance, availability, and security of those systems.
      iv. TIBCO conducts a security review of any third-party service TIBCO uses to deliver Software or a Cloud Service to ensure that such third party deploys industry appropriate measures to safeguard Protected Data.

   d. Personnel Management.

i. TIBCO regularly mandates information security training and awareness to employees and permitted subcontractors (collectively "Personnel"). TIBCO may impose disciplinary measures for Personnel that violate any of TIBCO's information security policies.

ii. All developers of Software delivered to Customers receive industry standard training in secure coding practices.

iii. TIBCO maintains employee completion reports of information security, code of conduct, and data management training. Upon written request, TIBCO will make available evidence of completion of Personnel training and qualifications, subject to any restrictions on the release of personal information pertaining to individual employees.

iv. TIBCO requires employees to use secure passwords for accessing systems that may contain Protected Data. Such passwords must (1) be changed regularly, (2) not reuse previously used passwords, (3) be at least eight characters in length and a combination of uppercase and lowercase letters, special characters, and numbers. Accounts will automatically lock after six failed attempts to gain access.

v. 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), require that such third parties implement policies and procedures that are at least as protective and as restrictive as those set forth in this Security Program in order to mitigate security risks and to ensure that appropriate controls and procedures are documented and followed.

vi. TIBCO conducts, in accordance with industry best practices and applicable laws, background checks for employees with access to Customer's physical premises, IT systems, or Protected Data. Subject to any local requirements, background checks may include (1) thorough background verification including whether the prospective employee has been convicted of a felony, property crime, or fraud in any state where the individual has resided, studied, or worked during the past seven years and (2) a check of United States' specially designated nationals list and the denied persons list. Further, TIBCO conducts due diligence reviews of all subcontractors that perform work for TIBCO on behalf of a customer, including checks against the designated nationals list and denied parties list.

vii. TIBCO removes access rights to critical systems and facilities that process Protected Data for all terminated employees and contractors within 24 hours of termination.

3. Data Protection

a. Data Protection Measures. TIBCO implements industry standard security measures to prevent unauthorized access to (i) physical premises and (ii) electronic systems that process Customer's Protected Data in the performance of (1) Maintenance (support services), (2) Consulting Services, and (3) a Cloud Service.

i. TIBCO strictly limits the processing of Protected Data to purposes stated in a written Customer agreement to accomplish a valid business purpose or to comply with governmental record retention regulations between TIBCO and the Customer. Further, TIBCO shall only make the minimum amount of Protected Data accessible on a need-to-know basis, limited to properly authenticated individuals. With respect to Maintenance and Consulting Services, Customers shall notify TIBCO before transmitting any Protected Data to TIBCO so that TIBCO may assess the appropriateness of receiving such Protected Data.

ii. For Protected Data that TIBCO is processing as part of a Cloud Service, TIBCO uses commercially available and industry standard controls and precautionary measures to ensure Protected Data is stored in a secure and encrypted environment based upon its classification.

iii. TIBCO implements, where available, an industry standard two-factor authentication system for certain applications that store Protected Data.

iv. TIBCO complies with applicable laws and regulations concerning the confidentiality, security, and processing of any Protected Data that it receives from Customer, including to the General Data Protection Regulation 20116/679 ("GDPR"), the EU Standard Contractual Clauses, the Health Insurance Portability and Accountability Act ("HIPAA"), and the California Consumer Privacy Act of 2018 ("CCPA").

v. If the GDPR applies to Protected Data that Licensor processes on behalf of Customer as a data processor, then the Licensor's Data Processing terms at https://terms.tibco.com/#data-processing-terms apply to such Protected Data.

vi. If TIBCO processes Protected Data that is 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, including 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.

1. 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 between TIBCO and the Customer and (ii) outside of the direct business relationship between TIBCO and Customer. Further, TIBCO shall not sell Protected Data that TIBCO processes under a Customer agreement for any reason. TIBCO certifies that it understands and will comply with the restrictions stated in this CCPA subsection.
2. For special classes of Protected Data, such as electronic Personal Health Information ("ePHI") or sensitive personal data, TIBCO requires special compartmentalized data handling and those administrative, physical and technical safeguards mandated by applicable regulations such as those issued under the HIPAA. Customers must notify TIBCO before transmitting any PHI or ePHI to TIBCO so that TIBCO may appropriately compartmentalize such data pursuant to this Security Program.

vii. Upon Customer's written request, TIBCO shall destroy or return any Protected Data in TIBCO's possession.

viii. Customer agrees to the terms of TIBCO's Privacy Policy (found at https://www.tibco.com/company/privacy and incorporated by reference), for any data submitted by Customer to TIBCO during the course of the business dealings between the parties.

b. Secure Data Transmission.

i. Any Customer Protected Data processed by TIBCO will be protected during transmission using industry accepted encryption and VPNs. Subject to a set of strict controls as dictated by TIBCO information technology team and the Security Group, TIBCO Personnel may access or store Customer Protected Data on mobile devices, tablets, or laptops.

ii. TIBCO utilizes and properly manages security infrastructure (e.g., firewalls, routers, IPS/IDS devices, load balancers, VPN concentrators) to control access between the internet and a Cloud Service by containerizing & segmenting access by security profiles to controlled networks and private clouds and only allowing authorized traffic.

c. Incident Management.

i. For purposes of this Security Program, a "Security Incident" means any known or suspected impairment to the security of Protected Data, including any (1) act or omission that violates any law, industry requirement, TIBCO's internal policies, or the Security Program or (2) unauthorized access to, loss, alteration, or disclosure of Customer's Protected Data. TIBCO has an established set of procedures that requires Personnel to promptly report actual and/or suspected Security Incidents.

ii. TIBCO's Security Group identifies, investigates, and assesses the seriousness and extent of each Security Incident; mitigates the effect of a Security Incident; conducts root cause analysis; implements and documents remedial action plans; and prevents the recurrence of similar incidents.

iii. TIBCO applies industry standard monitoring and logging technologies to record relevant actions involving attempts to access TIBCO's computing systems or Customer Protected Data. Security Incidents that do not compromise any Protected Data are securely logged on TIBCO's systems, are reviewed regularly, and maintained for a minimum of twelve months.

iv. TIBCO will promptly notify the designated Customer security contact of any Security Incidents that compromise Customer's Protected Data. The notice will state the approximate date and time of the occurrence and other relevant information about the Security Incident.

d. Storage, Back-up, and Deletion

i. As a multinational corporation, TIBCO stores and accesses certain Customer Protected Data across global locations. TIBCO performs risk assessments to identify and mitigate risks to Protected Data from such storage and/or access while taking into consideration geopolitical sensitivities that are not solely governed by economic considerations.

ii. TIBCO does not permit the storage of any Protected Data, with the exception of business contact information, on TIBCO issued portable devices such as laptops and smart phones unless those devices are encrypted using strong encryption and are configured with remote wipe and remote shutdown capabilities.

iii. TIBCO regularly backs up systems used to provide a Cloud Service to Customers to ensure data is available. Backups are appropriately classified according to TIBCO's internal data classification definitions and protected to ensure only authorized individuals are able to access the Protected Data, including but not limited to data stored off-site in electronic media and protection of hard copy records.

iv. TIBCO disposes of both tangible property and electronic files containing Protected Data according to the Department of Defense Standard DoD 5220.22-MM.

v. TIBCO shall stop Processing the Protected Data and, at the election of Customer, either return or delete all copies of Protected Data once TIBCO no longer needs the Protected Data to perform the services agreed to by the parties.

4. Product and Infrastructure Security

a. TIBCO complies with secure software development practices consistent with industry accepted standards and practices. As a general practice, TIBCO:

i. Restricts access to source code to authorized users who have a direct need to know.

ii. Performs quality control and security management oversight of all software development.

b. Network Security. TIBCO uses industry standard enterprise vulnerability management solutions to regularly scan TIBCO’s network for known vulnerabilities that are capable of generating alerts containing sufficient information to detect and evaluate potential incidents. Further, TIBCO uses industry standard firewalls to segment and protect the organization's internal network from the internet to protect such systems and applications from outside threats and also to segregate systems that process Customer Protected Data from other less restricted internal networks and systems.

c. Security Monitoring and Remediation. TIBCO regularly (but not less than annually) tests and monitors its controls, systems, and network to validate proper implementation and effectiveness in addressing the threats, vulnerabilities, and risks identified. This testing and monitoring may include: (i) internal risk assessments; (ii) formal procedures such as port scans, testing, and validation of multi-factor authentication for select environments; (iii) third party compliance, including hosting services and third party components; (iv) penetration testing; and (v) assessing changes affecting systems processing authentications, authorizations, and audits.

d. Vulnerability Management.

. TIBCO enables and keeps current trusted, commercially available anti-virus software to protect TIBCO controlled servers and systems, including those servers and systems used in accessing, processing, transmitting, or storing Protected Data, and requires the same from third party suppliers’ servers and systems subcontracted by TIBCO to perform services.

i. TIBCO scans for vulnerabilities using accepted industry practices, standards, protocols and monitors vulnerabilities reported by third parties.

ii. TIBCO uses trusted, current, and commercially available endpoint protection on TIBCO’s PC’s.

e. Patch Management.

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

ii. Customers with a current Maintenance entitlement for Software may obtain security patches made generally available by TIBCO in response to any known vulnerabilities.

f. Penetration Testing. TIBCO performs periodic vulnerability assessments on TIBCO’s applications and systems. Application testing includes both automated analysis and manual assessment. Where appropriate, each vulnerability detected by the Supplier shall have a unique common vulnerability and exposure identifier associated with a common vulnerability scoring system “(CVSS”) score (v2 or higher). Any “very high”, “high”, or “medium” severity vulnerabilities and any vulnerabilities with CVSS ratings higher than 7.0 are promptly remediated and retested for verification.

5. Business Continuity and Disaster Recovery

a. TIBCO maintains business continuity and disaster recovery plans to enumerate procedures for the continuity, recovery, and operation of information systems and facilities that could impact any application or system directly associated with the accessing, processing, storage, communication or transmission of Protected Data (“DR Plan”).

b. 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, outbreak of disease, 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 measures, including documenting the tests in writing.

6. **Customer Access and Review.** Upon reasonable prior written notice by Customer; subject to TIBCO's confidentiality and security conditions and execution of a mutually agreed upon NDA applicable to the audit; and pursuant to the agreement between TIBCO and Customer that governs any specific rights to access or audit TIBCO's policies or facilities, TIBCO may make its security policies, procedures, and other security-related information related to Customer's Protected Data or licensed Software available for Customer's review. TIBCO reserves the right to require its prior written approval to any third-party review of the DR Plan, and to impose reasonable conditions and restrictions on such third party access.