www.tibco.com

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
Tel: +1 650-846-1000
Toll Free: 1 800-420-8450
Fax: +1 650-846-1005

TIBCO Service Provider Security Standards

Rev. 2-20160509

Table of Contents

1. Introduction

Every TIBCO Service Provider is responsible for protecting TIBCO Assets and must take care to ensure that TIBCO Assets are not misappropriated, loaned to others, disposed of, sold or donated, without appropriate authorization. All TIBCO Service Providers are responsible for the proper use of TIBCO Assets, and must safeguard such assets against loss, damage, misuse or theft. Service Providers who violate any aspect of these Standards or who use poor judgment in the manner in which they use any TIBCO Asset may be subject to termination of their agreement and business relationship with TIBCO at TIBCO's sole discretion. TIBCO Assets are to be used for TIBCO business purposes only. Service Providers may neither make personal use of TIBCO Assets, nor may they allow any other person to use TIBCO Assets. Each Service Provider is responsible for compliance with the terms of these Standards by its employees and agents. If requested, a Service Provider will certify to TIBCO in writing its compliance with these Standards.

Additional security requirements may be specified in the agreement between TIBCO and the Service Provider. Where such additional security requirements are supplemental to those contained in these Standards, both sets of requirements shall apply; where a security requirement in an agreement conflicts with one contained in these Standards, the more stringent requirement shall apply.

2. Definitions

"Non-Public Information" or "NPI" as used in these Standards means any information held by TIBCO, either on its own behalf or on behalf of a customer or other third party, that has not been publicly disclosed by an authorized representative of TIBCO. NPI includes, but is not limited to, intellectual property, financial information, corporate plans or strategies, customer relationship information, Personally Identifiable Information (also referred to as PII), Protected Health Information (also referred to as PHI), electronic Protected Health Information (also referred to as ePHI), and, unless stated otherwise in writing by TIBCO, all TIBCO customer information held or processed by TIBCO. In the context of individuals, NPI includes, but is not limited to, any piece of information which can potentially be used uniquely to identify, contact, or locate a specific person such as an individual's:

- Full name, or a component of a person's name when associated with other information that makes identification of a person possible
- National identification number (for example, Social Security Number)
- Telephone number
- Street address
- E-mail address
- IP address (in some cases)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Bank account information
- Credit card numbers
- Passport information

- Insurance information
- Medical record information
- Familial information
- Detailed demographic information
- Digital identity

"Service Provider" as used in these Standards means any contractor, vendor, supplier, agent, consultant or other third party engaged by TIBCO as an independent contractor.

"TIBCO" as used in these Standards means TIBCO Software Inc. and its affiliates or subsidiaries.

"TIBCO Assets" as used in these Standards means any TIBCO Confidential Information and Information Systems defined in an agreement between you and TIBCO; it also includes any TIBCO provided equipment, facilities, software, office or work supplies, and NPI, and any other tangible or intangible thing which, by its nature, would be understood by a reasonable person as being confidential to, or an asset of, TIBCO.

3. Use of TIBCO Information Systems

To the extent Service Provider is granted access to TIBCO Information Systems (issued a password and/or other access credentials and/or mechanisms and/or a TIBCO User ID), Service Provider shall comply with these standards and any additional security or usage policies instituted or enforced by TIBCO's information technology, cybersecurity or other responsible offices.

3.1 Information System Networks and Environments

When accessing Information Systems over the Internet, Service Provider may use only (i) encrypted network traffic via an industry-standard Virtual Private Network (VPN) or equivalent technology, or (ii) other means which may be specifically authorized by TIBCO (e.g., direct dial-up or DSL if permitted) and specified in the agreement. Unless otherwise specified in the agreement, connections to TIBCO Information Systems will be provided by TIBCO utilizing a VPN connection.

Service Provider may not use or permit use of TIBCO's environments or networks for any purpose that may: (a) menace or harass any person or cause damage or injury to any person or property; (b) involve the publication of any material that is false, defamatory, harassing, or obscene; (c) violate privacy rights or promote bigotry, racism, hatred or harm; (d) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (e) constitute an infringement of intellectual property or other proprietary rights; or (f) otherwise violate applicable laws or regulations.

3.2 Passwords

- For TIBCO Information Systems where connections are via VPN, password rules shall be enforced by TIBCO through ActiveDirectory.
- Passwords must conform to strong password standards that include length, complexity, and expiration. Passwords must not be written down or stored on-line unencrypted.
- Passwords may not be shared. Each Service Provider employee or agent to whom access is granted must be provided a unique identifier and password for the networks and environments.
- Any passwords stored online will be stored using cryptographic hashing.
- Service Provider will change passwords on a regular basis; use of any one password may not exceed 90 days.
- Service Provider will abide by any further requirements provided by TIBCO for passwords on any TIBCO or client computer, network or environment.

4. Computer Protection

4.1 Virus Controls

Service Provider will employ the following computer virus controls for all computers:

- Scan all e-mails sent both to and from any recipient for malicious code and delete email attachments that are infected with known malicious code prior to delivery.
- Use industry-standard virus protection software. Virus definitions must be updated regularly (in no event to exceed 7 days).
- Automate virus updates, which may not be disabled.

4.2 Patches

When security patches are issued for operating systems and software, such patches must be applied promptly on all relevant computers. Computers should be configured to automatically receive such security patches when issued.

5. Physical Security

5.1 Service Provider Premises

If a Service Provider location has access to TIBCO Assets or Information Systems (the “service locations”), Service Provider agrees that it will, at each such location:

- limit access to its employees and other authorized personnel;

- monitor and properly manage the possession of keys and access cards and the ability to access the location;
- require all visitors to sign a visitor's register and be escorted or observed when on the premises of the location;
- issue identification cards that Service Provider employees and authorized personnel must wear while on the premises of the location; and
- prohibit photographic or other recording of any type (including cell phones, tape recorders, and video recorders) in and around computers that can access TIBCO Assets or Information Systems.

5.2 TIBCO Premises

TIBCO has and will continue to develop procedures covering physical access control to ensure privacy of communications, security of TIBCO communications equipment, and safeguarding of TIBCO Assets. Each representative of a Service Provider is personally responsible for complying with the level of access control that has been implemented at the TIBCO premises where Service Provider will work.

Service Providers should not maintain any expectation of privacy with respect to information transmitted over, received by, or stored in any electronic communications device owned, leased, or operated in whole or in part by or on behalf of TIBCO. To the full extent permitted by applicable law, TIBCO retains the right to gain access to any information received by, transmitted by, or stored in any such electronic communications device, by and through its employees, agents, Service Providers, or representatives, at any time, either with or without an employee's or third party's knowledge, consent or approval. When visiting or working at TIBCO premises, Service Provider is required to abide by TIBCO's building and facilities security requirements and any direction provided by TIBCO.

5.3 TIBCO Badges/Passcards

Service Provider Badges: TIBCO Facility Security may issue badges/passcards to new local Service Providers working on TIBCO premises by taking a digital photo which is then printed and applied to the access badge. A Service Provider badge will include an expiration date after which the badge will no longer function.

In the event "day use only" badges/passcards are issued for local Service Providers, TIBCO may exchange the TIBCO badge for Service Provider personal identification (e.g., a driver's license, passport, or credit card) or vehicle keys (to encourage returning of the badge after completion of their visit).

Immediately upon termination or resignation of any Service Provider employee or agent, or Service Provider learning of the death of its employee or agent, Service Provider must take appropriate actions to terminate any access that had been granted to said employee or agent to computers, networks, and environments, as well as physical access to service locations.

TIBCO affiliate and subsidiary premises may have different badge/passcard and security procedures. Service Provider shall adhere to all badge/passcard and security procedures relevant to the premises that it is accessing.

5.4 TIBCO Customer Premises

If Service Provider is performing services at a TIBCO customer's premises, Service Provider is responsible for obtaining and adhering to all of the TIBCO customer's policies, procedures and standards, as well as TIBCO's own standards.

6. Confidentiality, Privacy and Data Protection

The passwords for the networks and environments, and all NPI and other data are TIBCO's confidential information. Service Provider will provide its employees and agents access to the networks, environments and any NPI only on a need to know basis, and may not disclose any NPI to any third party without TIBCO's prior written consent. Service Provider is responsible for ensuring that its employees' and agents' access, use, and protection of the service locations, computers, networks, NPI, data, environments, all TIBCO Assets, and other confidential information are consistent with the terms of its agreement with TIBCO, all applicable laws and regulations, and these Standards.

As a means to ensure the protection of NPI and other data, Service Provider agrees that it will:

- Access, use and process NPI and other sensitive data only on behalf of TIBCO and only for the purposes specified in Service Provider's agreement with TIBCO, in compliance with these Standards and such further instructions as TIBCO may provide regarding the processing of such NPI and other data;
- Inform TIBCO promptly if Service Provider has reason to believe that legislation applicable to Service Provider (or changes in legislation applicable to Service Provider) prevent it from fulfilling the obligations relating to treatment of NPI or other data under these Standards and/or Service Provider's agreement with TIBCO; and
- Notify TIBCO immediately and, to the extent permitted by law, act only upon TIBCO's instruction concerning any request:
- for disclosure of the NPI or other data by a law enforcement officer or other governmental authority;
- by law enforcement or other governmental authority for information concerning the processing of PII or other data in connection with this Agreement; or
- received directly from an individual concerning his/her PII, PHI or ePHI.

In addition to this Standard, Service Providers performing services at a TIBCO customer site shall comply with the terms of TIBCO's Customer Privacy and Security Statement, published at http://www.tibco.com/customer_privacy_security_statement.jsp and the Data Protection Policy Statement at http://www.tibco.com/resources/data_protection_statement.pdf, the terms of the agreement with TIBCO, as well as any customer policies, procedures and standards, and any applicable laws or regulations regarding the protection of PII.

Service Provider will employ clean-desk and clear-screen policies (i.e., policies and practices designed to restrict physical and logical access to confidential information on a need-to-know basis) to protect all data and other confidential information.

Service Provider must immediately report to TIBCO (i) any security or other event that creates reasonable suspicion of unauthorized access to TIBCO NPI or an environment, and/or the misappropriation or alteration of any NPI; and (ii) the loss or theft of any computer, device or media believed to contain TIBCO Assets, including but not limited to NPI. Service Provider will take appropriate steps to address any such incident immediately, and will follow any additional instructions TIBCO provides with respect to such incident and/or remediation identified in response to such incident.

7. Monitor and Audit

Service Provider will maintain a complete list of all individuals, including but not limited to their geographic location, address, and citizenship, with permission to access the TIBCO Assets, including its networks, environments and/or data.

To the extent permitted by law, TIBCO may monitor Service Provider's access to and use of the environments and networks. TIBCO also may perform security audits upon reasonable notice to confirm compliance with these Standards.