Wabtec Third Party Information Security Requirements

INTRODUCTION

The Wabtec Third Party Information Security Requirements document outlines the security requirements applicable to Wabtec Third Parties, including suppliers and joint ventures. The security requirements outlined herein are applicable to Third Parties that Process Wabtec Confidential Information, have access to a Wabtec Information System, or provide certain services or Products, as described below. The security requirements are designed to vary based on the level of risk the Third Party Products or services may present to Wabtec.

Wabtec reserves the right to update this document from time to time.

SECTION I - MINIMUM SECURITY REQUIREMENTS

If a Third Party Processes Wabtec Data or Wabtec Confidential Information, or has a Direct Network Connection to the Wabtec managed network, the Third Party shall, at a minimum, do or implement the following:

Minimum Security Requirements
Written policies and procedures addressing information security, including roles and responsibilities
Accurate inventory of assets, including those that Process Wabtec Data or connect to Wabtec managed network
Security Education Training and Awareness Program to ensure workers receive regular security awareness training
Access Management Program that ensures that access to information systems, or data contained therein, is approved prior to being granted, access credentials are appropriately secured and managed to limit access to those with a legitimate business need, and Third Party's personnel's access to both Wabtec's systems and Third Party's systems is immediately revoked once there is no longer a legitimate business need for such personnel to access those systems or information contained therein.
Passwords and other pass-phrases that are of sufficient complexity and re-use, managed consistent with industry expectations
Authentication mechanism or process to protect and validate access to systems or information including timeouts and limiting failed attempts
Physical security of offices, rooms, facilities and all communication networks against external and environmental threats
Network environments that separate production and non-production systems
Industry Best Practices for network protection (i.e., Intrusion Detection, Intrusion Prevention, Data Loss, Firewalls), which are monitored where applicable
Logs of security events; logs must be kept secure
Third party risk management program that ensures services and Products are provided in a secure manner and company information is managed securely
Incident Response Program to ensure timely response, reporting and management of incidents
Periodic independent reviews of the security management program that are conducted by management and identified risks are tracked and decisioned
Vulnerability Management Program to identify and remediate vulnerabilities in all systems, products, services, network devices, etc., in an effective and timely manner.

If applicable, Secure Development Lifecyle expectations regarding code management, change management, and code reviews for software and systems used internally or provided to Wabtec
Secure disposal and re-use processes that are aligned with industry standard procedures to ensure information is destroyed
Documentation of data flows for all Wabtec Confidential Information within the Third Party's control
Business Continuity, Disaster Recovery, and Capacity Management plans to ensure continued delivery of services
Secure transmission, including use of encryption, of information or data; information or data at rest must be secured.

SECTION II - SOFTWARE OR PRODUCT DEVELOPMENT SECURITY CONTROLS

In addition to any applicable Minimum Security Requirements (listed in Section 2 above), a Third Party that develops Products for, or provide Products to, Wabtec shall do or implement the following:

Software or Product Development Security Controls
Secure software development lifecycle policy, detailing "security by design" and "privacy by design" concepts
Security testing processes to ensure that all developed Products undergo predefined security testing and formal acceptance to meet Wabtec's needs
Security training provided to Product developers on how to incorporate "security by design" and "privacy by design" into Products, including how to identify and address security vulnerabilities and flaws
Secure development tollgates must be documented and followed to ensure appropriate reviews and approvals throughout the entire software development lifecycle processes
All source code and 3rd party libraries must be periodically scanned for vulnerabilities; Systems or services used for these scans must be disclosed to Wabtec prior to code development
All vulnerabilities deemed "Critical", "High" or "Medium", per the Common Vulnerability Scoring System, must be remediated before delivery to Wabtec. All remaining vulnerabilities must be reported to Wabtec upon delivery of any software code or 3rd party libraries
Third Party represents, warrants and covenants that (i) it has disclosed all Open Source Software and Third Party Materials utilized with the Products, and no Open Source Software or Third Party Materials have been or will be provided to Wabtec or used as a component of or in relation to any Products provided under the Contract Document, except with the prior written authorization of Wabtec; and (ii) all Open Source Software contained within the or Products are and shall be in material compliance with the terms and conditions of the applicable licenses governing their use, and the Products or the use thereof by Wabtec shall not cause Wabtec or Wabtec's intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require Wabtec to fulfil any open source license obligations for any Open Source Software contained within the Products.
A threat model is required for all software systems that are developed for Wabtec
Third party will not engage other third parties that have access or will create software for Wabtec without prior approval
Systems used in the development of software or Product must be free of vulnerabilities; Third Party must not use obsolete or unsupported software or systems in the development of Product

Cybersecurity guidance in the documentation provided to Wabtec regarding use of Product. This documentation shall include guidance on how to configure Products and/or the surrounding environment to best ensure security
If any cryptographic systems are contained in the Product, Third Party shall only use cryptographic algorithms and key lengths that meet or exceed the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-131A, and Third Party shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity
Third Party must develop and maintain an up-to-date Cybersecurity Vulnerability management plan designed to promptly identify, prevent, investigate, and mitigate any Cybersecurity Vulnerabilities and perform any required recovery actions to remedy the impact with respect to Products provided to Wabtec.
Third Party shall notify Wabtec within a reasonable period, in no event to exceed three (3) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability impacting a Product provided to Wabtec. Third Party shall report all critical Cybersecurity Vulnerability that would have a significant adverse effect on Wabtec and any Cybersecurity Vulnerability with a fix to Wabtec at security@waptec.com with "Vulnerability Notice" in the subject line, or at such contact information communicated to Third Party from time to time. Within a reasonable time thereafter, Third Party shall provide Wabtec, free of charge, with any upgrades, updates, releases, maintenance releases and error or bug fixes necessary to remediate any Cybersecurity Vulnerability. Third Party shall reasonably cooperate with Wabtec in its investigation of a Cybersecurity Vulnerability, whether discovered by Third Party, Wabtec, or another third party, which shall include providing Wabtec a detailed description of the Cybersecurity Vulnerability, the remediation plan, and any other information Wabtec reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. Wabtec or Wabtec's agent shall have the right to conduct a cybersecurity assessment of the applicable Software or Products, and the development lifecycle, which includes tests intended to identify potential cybersecurity vulnerabilities. Third Part shall designate an individual responsible for management of the Cybersecurity Vulnerability and shall identify such individual to Wabtec promptly.
Third Party represents, warrants, and covenants that the Products: (a) do not contain any restrictive devices such as any key, node lock, time-out, time bomb, or other function, whether implemented by electronic, mechanical, or other means, which may restrict or otherwise impair the operation or use of the Products or any material embodying or comprising Software or Products; and (b) shall be free of viruses, malware, and other harmful code (including, without limitation, time-out features) which may interfere with the use of the Software or Products regardless of whether Third Party or its personnel purposefully placed such code in the Products. In addition to exercising any of Wabtec's other rights and remedies under this Agreement or otherwise at law or in equity, Third Party shall provide Wabtec, free of charge, with any and all new versions, upgrades, updates, releases, maintenance releases, and error or bug fixes of the Software or Products which prevents a breach of any of the warranties provided under this Agreement or corrects a breach of such warranties.
When a data storage device is decommissioned the device must be data sanitized using documented industry standard procedures

SECTION III - DATA CENTER SECURITY CONTROLS

In addition to any applicable Minimum Security Requirements (listed in Section 2 above) a Third Party that provides data center facility services to, or on behalf of, Wabtec shall do or implement the following:

Data Center Security Controls
Periodic third-party attestation of documented, effective and complete controls covering physical security, access management, environmental security, utility resilience, segregation of tenants' assets, ongoing monitoring, and maintenance of all appropriate systems
A documented process for delivery or handling of equipment or media
Data centers that have a disaster recovery plan for the facility and environment that at least identifies and mitigates risks to Wabtec services in the event of a disaster. The plan shall provide for contingencies to restore facility service if a disaster occurs, such as identified alternate data center sites. The plan shall be shared with Wabtec to ensure Wabtec can coordinate with its own data recovery plan

SECTION IV - DIRECT NETWORK CONNECTIVITY TO WABTEC NETWORK CONTROLS

In addition to any applicable Minimum Security Requirements (listed in Section 2 above), a Third Party that has a persistent or routable connection to a Wabtec network shall do or implement the following:

Direct Network Connectivity to Wabtec Network Controls
Third party shall use only Wabtec managed network devices to connect to the Wabtec Network. Wabtec requires out of band connectivity to the remote device for administration. Wabtec must approve all methods of connectivity before connections are established
Third party shall ensure that no employees will circumvent or disable any security measures put in place by Wabtec
If Wabtec notifies the Third Party of any confirmed "High" or "Critical" vulnerabilities relating to Third Party's connection to Wabtec networks, the Third Party shall remediate the confirmed vulnerability within 30 days

DEFINITIONS

Contract Document means the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of Products, services and/or deliverables by Third Party to Wabtec.

Controlled Data is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export-controlled data, which is provided by Wabtec to the Third Party in connection with performance of the Contract Document.

Copyleft License means the GNU General Public Licenses version 2.0 (GPLv2) or version 3.0 (GPLv3), Affero General Public License version 3 (AGPLv3), or any other license that requires, as a condition of use, modification and/or distribution of or making available over a network any materials licensed under such a license to be: (a) licensed under its original license; (b) disclosed or distributed in source code form; distributed at no charge; or (d) subject to restrictions on assertions of a licensor's or distributor's patents.

Cybersecurity Vulnerability (ies) means any bug, software defect, design flaw, or other issue with software associated with a Product that could adversely impact the confidentiality, integrity or availability of information or processes associated with the Product.

Direct Network Connection is inclusive of all manners to connect to the Wabtec network through any persistent connection including site-to-site VPN solutions.

Wabtec Confidential Information is information created, collected, or modified by Wabtec that would pose a risk of causing harm to Wabtec if disclosed or used improperly, and is provided to the Third Party under the Contract Document. Wabtec Confidential Information includes, but is not limited to, information pertaining to business operations and strategies, trade secrets, Personal Data, Controlled Data, or Sensitive Personal Data.

Wabtec means the Westinghouse Air Brake Technologies Corporation or a Wabtec Affiliate party to the Contract Document with Third Party.

Wabtec Affiliate means any entity that is directly or indirectly in control of, controlled by, or under common control with Wabtec, whether now existing, or subsequently created or acquired during the term of the Contract Document.

Wabtec Data includes all data provided to Third Party by Wabtec or on behalf of Wabtec as a result of a Contract Document or services being provided to Wabtec by Third Party. Wabtec Data includes Confidential, Personal, Controlled, or Sensitive Personal Data.

Wabtec Information System(s) means any systems and/or computers managed by Wabtec, which includes laptops and network devices.

Highly Privileged Accounts (Users), or HPAs, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system, security, or application controls.

Mobile Devices means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

Open Source Software means any material that is distributed as "open source software" or "freeware" or is otherwise distributed publicly or made generally available in source code form under terms that permit modification and redistribution of the material on one or more of the following conditions: (a) that if the material, whether or not modified, is redistributed, that it shall be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; and/or (iii) distributed at no charge; (b) that redistribution must be licensed or distributed under any Copyleft License, or any of the following license agreements or distribution models: (1) GNU's General Public License (GPL), Lesser/Library GPL (LGPL), or Affero General Public License (AGPL), (2) the Artistic License (e.g., PERL), (3) the Mozilla Public License, (4) Common Public License, (5) the Sun Community Source License (SCSL), (6) the BSD License, (7) the Apache License and/or (8) other Open Source Software licenses; and/or (c) which is subject to any restrictions on assertions of patents.

Personal Data means any information related to an identified or identifiable natural person (Data Subject), as defined under applicable law Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law.

Product(s) mean any goods, systems, components, products, software and deliverables supplied under the Contract Document.

Process(ing) means to perform any operation or set of operations upon Wabtec data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

Sensitive Personal Data is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance and Portability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation).

Significant Change or Enhancement (to software) means:

- Any code change that impacts application interfaces (modifies data stream inputs/outputs).
- Any code change to the application that modifies access to or use of external components (database, files, DLLs, etc.).
- Any code change that impacts access control.
- A complete or partial rewrite of an application into a different language (ex. C++ to Java) or different framework (ex. Struts and Spring).
- A change in the application that results in internet exposure where previously it was not.
- A change in the application that results in the Risk Level increasing (ex. reclassification from Level 4 to Level 3).
- Transferal of development responsibilities from one Third Party to another, from a Third Party to Wabtec, or from Wabtec to a Third Party. The correction of any existing critical or high vulnerabilities must be conducted prior to transfer or included in the work order for the new Third Party to correct within the applicable remediation timeframe.

Third Party or Supplier is the entity that is providing goods or services to Wabtec pursuant to the Contract Document. It also refers to Wabtec joint ventures.

Third Party Information System(s) means any Third Party system(s) and/or computer(s) used to Process, Store, Transmit and/or Access Wabtec Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

Third Party Materials means materials which are incorporated by Third Party in any Products provided to Wabtec, the proprietary rights to which are owned by one or more third party individuals or entities.

Third Party Personnel means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates and third parties (for example, suppliers, contractors, subcontractors, and agents), as well as anyone directly or indirectly employed, engaged or retained by any of them.

Trusted Third Party Network Connection is a physically isolated segment of the Third Party network connected to Wabtec internal network in a manner identical to a standard Wabtec office.