Wabtec Product Cybersecurity Appendix

Version: 1.0

Effective Date: September 3, 2026

1. INTRODUCTION

The Wabtec Product Cybersecurity Appendix outlines the minimum viable security controls applicable to Wabtec third parties, including Suppliers and joint ventures, who create, Process, store, or transmit Wabtec or Personal Data, and/or have logical access to Wabtec information system, and/or provide certain products or services. The security requirements are subject to vary based on the level of risk of the Third-Party products and/or services inherent to Wabtec.

These minimum-security requirements are categorized based on the intended use of the component:

- **Products for Use With Wabtec Customers**: Applicable to products or components that will be integrated into a Wabtec offering made available to customers, either as part of a larger product or as a resale product.

Wabtec reserves the right to update this document as needed.

2. MINIMUM SECURITY REQUIREMENTS

If a Third-Party creates, Processes, transmits, or stores Wabtec or Personal Data and/or employed digital connectivity to Wabtec managed network, then the Third-Party shall, at minimum, meet or oblige to be compliant to the minimum-security controls defined below:

Minimum Security Requirements
Written policies and procedures addressing information security, including roles and responsibilities
Accurate inventory of Assets, including those that Process Wabtec or Personal Data or connect to Wabtec managed network
Security awareness training to ensure employees and/or contractors receive regular security awareness training
Access management measures ensuring, i) access to information systems, or data contained therein, is approved prior to being granted ii) access credentials are appropriately secured and managed to limit access to only those with a legitimate business need iii) 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 passphrases that are of sufficient complexity and re-use are managed consistently 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 known and acceptable practices for network protection (e.g., Intrusion Detection, Intrusion Prevention, Data Loss, Firewalls), which are monitored regularly
Logs of security events are enabled and kept secure
Third-Party risk management program that ensures services and products are provided in a secure manner and company information is managed securely
Third-Party must enforce pre-engagement screening for any personnel engaged by or on behalf of a Third-Party to perform any services, including employees, contractors, and subcontractors of the Third-Party or Third-Party affiliates.
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 lifecycle 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 or Personal Data within 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

3. 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 provides products to Wabtec, shall implement the following:

Products for Use With Wabtec Customers
Certifications
A Supplier must provide information on relevant security certifications and must be able to show how their SDLC aligns with the IEC 62443-4-1 and 62443-4-2 and identify any gaps. Relevant security certifications may include IEC 62443-4-1, ISO/IEC 27034-1, NIST CSF, or other specific security frameworks.
Secure Development Lifecycle (SDLC)
A Supplier shall • Integrate security considerations into all phases of the product development lifecycle ("Security by Design"). • Document processes for managing security vulnerabilities and incidents throughout the product lifecycle. • Define roles and responsibilities for product security personnel.

- Implement software configuration management processes, including change controls and audit logging.
- Ensure security-related findings related to products identified during development are addressed and tracked to closure.
- Use specific tools such as SAST, OSS Scanning, DAST etc., or industry-recognized methodologies to support the SDLC.

Threat Modeling

A Supplier shall

- Conduct and update threat modeling exercises to identify potential product vulnerabilities and security risks.
- Identify potential attack vectors and conduct risk analysis for each.
- Manage mitigation to all threats until closure.
- Create and regularly maintain a threat database relevant to the products being sold.
- Review the threat model yearly and update the threat database periodically.

Security Requirements

A Supplier shall

- Define product security requirements based on security classification. Manage all security requirements to ensure pertinent security capabilities, including access control, authentication, authorization, auditing, and secure communication.
- Ensure all product security requirements related to installation, configuration, operation, maintenance, and decommissioning are met.
- Validate, through documentation, product security requirements throughout the development lifecycle.
- Manage changes to product security requirements during the secure development lifecycle.

Secure Coding Practices

A Supplier shall enforce appropriate secure coding standards for products (e.g., OWASP, CERT).

Vulnerability Management

A Supplier shall

- Prioritize and address vulnerabilities based on a risk scoring process.
- Monitor for and notify Wabtec's PSIRT of active exploitation of product vulnerabilities. Notifications can be sent to PSIRT@Wabtec.com.
- Release security patches and updates regularly (e.g., quarterly, every 6 months, yearly).
- Operate a product vulnerability disclosure program, providing vulnerability characteristics, impact, and risk mitigation and remediation guidance to customers.

Security Testing

A Supplier shall

- Perform appropriate types of product security testing, including fuzzing tests, security functional tests, dynamic application security testing (DAST), penetration testing, OSS Scanning, and static analysis.
- Conduct secure code reviews.

Release

- Ensure secure packaging, distribution, and delivery of products to avoid tampering and ensure the product is not compromised from the time it is produced to the time custody is transferred to Wabtec.

• Provide security-related documentation and guidance for secure installation, configuration, operation, and disposal of products.
Training and Awareness
A Supplier shall provide training for all product development personnel on product cybersecurity tailored to their roles and responsibilities.
Incident Response
A Supplier shall • Operate a product Security Incident response process, with reasonably monitored and externally accessible communication channels, that is regularly tested capturing lessons learned. • Make available an externally accessible method to receive and handle customer, researcher, or other entities, such as regulatory or governmental, reported security issues.
Continuous Improvement
A Supplier shall • Ensure continuous improvement of security practices and processes. • Use metrics to measure the effectiveness of security practices. • Incorporate feedback and lessons learned from past projects into security processes.
Supply Chain Security
A Supplier shall • Ensure Suppliers and subcontractors comply with secure development lifecycle policies and procedures set in place by their organization. • Identify and manage security risks of all externally provided components (e.g., open-source software, Third-Party components). • Monitor discovery sources for vulnerabilities in open-source software and Third-Party components, notifying Wabtec's PSIRT of those which are exploitable in the product. Additionally, including the discovered exploitable vulnerabilities in the disclosure program for communication downstream to customers.
Compliance Audits
Wabtec Product Security has the right to • Conduct regular cybersecurity compliance audits to evaluate adherence to IEC 62443 standards or other relevant security frameworks. • Perform penetration tests at Wabtec or through a third party to verify the security compliance of the provided component.
Regulations
A Supplier shall adhere to applicable cybersecurity regulations. For example, manufacturers of products with digital elements that will be made available on the European Union market shall comply with the European Union's Cyber Resilience Act (CRA).

4. 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 implement the following:

Data Center Security Controls
Third-Party shall ensure that Wabtec protected information is physically secured against unauthorized

access, including, but not limited to, by use of appropriate physical safeguards such as electronic ID card access to any areas of the Third-Party's information systems.
Hosting facilities, including buildings and infrastructure, must meet standards defined in ISO/IEC 27001 or NIST standards, including NIST SP 800-53, NIST SP 800-171 or the NIST Cybersecurity Framework (CSF), as agreed in writing following a security risk assessment undertaken by Wabtec or an independent Third-Party, as applicable.
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.

5. WABTEC NETWORK CONNECTIVITY SECURITY 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 implement the following:

Wabtec Network Connectivity Security Controls
The Third-Party shall maintain and keep current network component inventories, topology diagrams, data center diagrams, and internet protocol (IP) addresses for each network that connects to Wabtec information systems by: i) Ensuring network perimeter is protected by industry-leading enterprise firewall solutions, including port, protocol, and IP address restrictions that limit inbound/outbound protocols to the minimum required and ensure all inbound traffic is routed to specific and authorized destinations ii) Interrogating transmission control protocol (TCP) communications at the packet level to distinguish legitimate packets for different types of connections and to reject packets that do not match a known connection state, e.g., stateful inspection. This must consider network, application, and database protocols iii) Configuring perimeter systems with redundant connections to ensure there are no single points of failure iv) Interrogating communications by monitoring network packets to identify and alert upon or prevent known patterns that are associated with vulnerabilities or denial of service attacks with regularly updated signatures to generate alerts for known and new threats v) Maintaining and enforcing security procedures in operating networks that are at least consistent with industry standards for such networks and as rigorous as those procedures that are in affect for similar networks owned or controlled by the Third-Party vi) Maintaining and enforcing operational and security procedures that prevent provision of network connectivity to third parties, where such access would enable third parties' access to Wabtec protected information or information systems should network interconnections between the company and the Third-Party be enabled vii) Implementing perimeter management controls to ensure that perimeter systems are configured to be resistant to resource exhaustion (denial of service attacks), and viii) Keeping Wabtec protected information logically separated from all other Third-Party or Third-Party customer data/information.

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 with Wabtec, then Third-Party must remediate the confirmed vulnerability within 30 days.
Third Party shall conduct annual penetration testing, and after significant infrastructure or application changes affecting the Wabtec connection. Testing must be performed by qualified, independent professionals using recognized methodologies. The Third-Party shall provide Wabtec, upon request, with a summary of findings and remediation plans, and must remediate all "High" and "Critical" findings within **30 days**.

6. DEFINITIONS

Asset means owned or managed informational or physical asset; something of value to the organization. Includes managed information, systems, and network.

Business Continuity means the ability to maintain essential functions during and after a security incident.

CERT means Community Emergency Response Team

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; (c) distributed at no charge; or (d) subject to restrictions on assertions of a licensor's or distributor's patents.

Cybersecurity Vulnerability relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems, and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the nation.

DAST means Dynamic Application Security Testing

Disaster Recovery means a set of processes to resume normal operations after a security incident occurs.

Encryption means the act of converting information into code in order to prevent unauthorized access. The process of transforming readable data (plaintext) into a form that is unreadable (cipher text) by all except the authorized person(s) possessing the correct key to decrypt the data.

Malware means software such as viruses, worms, ransomware, and trojan horses. Code or executables containing malware can impact operations and access information by using active resources to self-replicate, gather sensitive data, or allow remote control, which may result in a breach of the system.

Open-Source Software [OSS] 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.

OWASP means Open Worldwide Application Security Project

Personal Data means any information that identifies, relates to, describes, is reasonably capable of being associated with or linked to a Data Subject and any information defined as "personally identifiable information," "personal information," "personal data" or similar terms as defined by applicable data protection laws.

Products for Use With Wabtec Customers: Applicable to products or components that will be integrated into a Wabtec offering made available to customers, either as part of a larger product or as a resale product.

Products for Wabtec Internal Use: Applicable to products or components intended solely for Wabtec's internal use.

Process(ing) means to perform any operation or set of operations upon Wabtec Data, whether 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.

PSIRT means Product Security Incident Response Team

SAST means Static Application Security Testing

SDLC means Secure Development Life Cycle

Security Incident (includes similar terms including "security breach", "incident', or Personal Data breach" as defined by any applicable data protection laws) is an occurrence that (1) actually or imminently jeopardizes, the integrity, confidentiality, availability, or is unauthorized access of information, an information system, or of protected data; (2) constitutes a violation or imminent threat of information system or data, security policies, security procedures, or acceptable use policies, (3) any actual or suspected unauthorized to or destruction, acquisition, loss, loss of access to, corruption or use of Personal Data.

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 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 or Supplier is the entity or individual that is not Wabtec, one of its subsidiaries, or Units. May be Joint Ventures (JVs) in which Wabtec has either majority ownership or has management control if not considered a subsidiary. May also include Wabtec customers, but only if that customer is also being engaged to provide goods or services to Wabtec.

Tollgate means a checkpoint or a control point used to manage access to secure areas of a system.

Wabtec Data includes all information and data of any type, form, or nature, excluding Third-Party Data, that is either contained in Wabtec Systems and/or Wabtec Networks or provided to a third-party, including customers or vendors, by or on behalf of Wabtec. Wabtec Data includes Wabtec Confidential Information and Wabtec Highly Confidential Information.

7. REVISION HISTORY

Date	Revision	Reason / Description
09/03/2026	1.0	Initial Published release