Information
Security Program Overview

Date of last review/update: 6/29/2026

Table of Contents

1. Introduction

J.B. Hunt Transport, Inc. (“J.B. Hunt” or the “Company”) is committed to protecting information, including personal data, and the information technology (“IT”) resources that store, transmit, and process that information, against incidents that could compromise its confidentiality, integrity, and availability, whether accidental, unlawful, or unauthorized, as well as from other unlawful forms of processing. Accordingly, the Company has implemented technical, organizational, and physical security measures designed to provide an appropriate level of information protection based on the risks associated with the processing and the nature of the information being protected. This document presents an overview of the digital information security measures and standards that J.B. Hunt applies globally.

J.B. Hunt may modify these technical, organizational, and physical measures from time to time, as long as such changes do not materially lower the level of protection and are not materially inconsistent with the protections described to its customers.

2. Requirements

2.1 Compliance

J.B. Hunt requires all employees who have access to Company data and IT resources (“Company Personnel”) to comply with the Company’s policies, procedures, and other safeguards designed to preserve information security.

2.2 Review and update process

Information security policies and procedures are subject to periodic review to ensure that they address any new technologies or threats.

Changes to existing policies and procedures, as well as the development of new ones, are subject to leadership review and approval, with oversight by a senior governance committee.

2.3 Communication of policies to employees

Company Personnel are made aware of information security policies and procedures at onboarding and through regular training.

Any exceptions to Company policies and procedures are subject to an established exception management process for approval and documentation.

2.4 Consistency with industry best practices

Systems and information designated for special handling, such as employee benefits or government data, comply with additional standards in accordance with applicable laws.

Annually, an independent third-party assesses the Company’s information security organization and its information security management program.

The Company conducts penetration tests for applications and networks and performs remediation for findings based upon the level of criticality.

2.5 Management of the information security program

An advisory committee made up of senior stakeholders provides guidance, counsel, and strategic oversight on key security and related compliance issues affecting J.B. Hunt.

Specialized teams are responsible for managing the Company's standards for security, addressing cybersecurity risks, providing security operations across the technical estate, and providing teams and leaders with security intelligence.

2.6 Training and awareness

Company Personnel are required to complete cyber security training on phishing and data privacy, as well as periodic training (at least annually) on other relevant topics, including the handling of confidential information.

The Company makes information about cybersecurity, data privacy essentials, and workplace security available to Company Personnel through its intranet site.

2.7 Office security controls

In addition to technical security controls, J.B. Hunt has implemented the following:

Company premises are subject to controls that limit physical access to Company Personnel and approved visitors.

J.B. Hunt offices implement protocols to manage and restrict visitor access, ensuring that visitors' presence is limited to designated areas and does not compromise the confidentiality of customer or employee information.

2.8 Data classification

To support appropriate protection of data on its systems, the Company uses a classification matrix that categorizes data based on sensitivity.

2.9 IT acceptable use guidelines

The Company has adopted policies on the acceptable use of Company technology. Controls have been implemented to reinforce appropriate behavior and prevent unauthorized use.

The Company's Code of Ethical and Professional Standards defines a set of expectations for the behavior of all Company Personnel regarding the protection of data.

The Company maintains risk-based procedures to lawfully review, monitor, and, where appropriate, disclose information communicated through its IT resources to help prevent, detect, investigate, and mitigate activities that may affect the security of its systems or Company and customer information, or that may be inconsistent with applicable policies, laws, or regulations.

Company Personnel are expected to apply mandated security controls to protect information stored in or transmitted through assigned IT resources and to share confidential information only with authorized recipients.

Company Personnel are prohibited from using unapproved software or services.

When traveling or working outside of J.B. Hunt facilities, Company Personnel are required to take measures to protect assigned equipment against theft and to report lost or stolen devices immediately.

2.10 Authentication and access management

The Company's policy is to grant Company Personnel only that level of access to data that is appropriate to their role and responsibilities.

J.B. Hunt honors the principle of segregation of duties to reduce opportunities for unauthorized modification or misuse of information or services.

The Company implements Active Directory password controls that align with the guidelines of NIST SP800-63-3.

Company devices, applications, and systems are configured to automatically log off or lock a user's session if there is no keyboard, mouse, or touchscreen activity for a defined period of time.

Access to Company computers and mobile devices is disabled after multiple consecutive unsuccessful logon attempts.

J.B. Hunt has implemented procedures for disabling and removing accounts that are no longer in use, subject to applicable legal, regulatory, or operational requirements.

Additionally, when Company Personnel separate from the Company, their access to digital information, including computing and communications resources that store or process information, is terminated in accordance with a documented process.

2.11 Change management

The Company maintains a change management process designed to minimize the impact of change on operational stability, ensure transparency around change activities, account for rollback procedures, and promote efficiency and agility for both standard and emergency changes.

2.12 Data centers

To protect digital information at rest, in-transit, and in use, the Company maintains an IT infrastructure designed to adhere to industry best practices. Key aspects of the infrastructure include the following:

Physical access is granted to only those individuals with a legitimate business need. Data centers are physically protected by multiple layers of security (e.g., biometric access controls, CCTV cameras, and on-site security officers).

Data is not permitted to leave the data centers unless it is protected by strong encryption, whether stored on encrypted tapes or other encrypted portable media, or transmitted through encrypted telecommunications channels.

J.B. Hunt has implemented measures designed to ensure that information collected for different purposes is segregated and processed separately, including, where appropriate, through logical separation of confidential information.

2.13 Software and network

J.B. Hunt uses firewalls, filters, access-control lists, intrusion-detection software, and anti-malware software to protect its products and networks against external digital threats and from unauthorized interception, monitoring, or modification.

J.B. Hunt product development follows an established development lifecycle process, which employs multiple testing procedures (including design and code reviews, as well as functional and penetration tests) to mitigate potential vulnerabilities before the product goes live, and periodically thereafter.

Production and non-production environments are segregated. Promotion from a non-production environment to the production environment must follow an established change management process.

J.B. Hunt secures access to its wireless networks within its offices through security controls that include a single sign-on solution (SSO) and multi-factor authentication (MFA).

Servers and network devices undergo vulnerability scanning at least monthly. Findings are divided into risk categories (i.e., critical, high, medium, low) and are addressed within the time frame prescribed for the respective category.

On-going scanning for unauthorized devices is conducted by using technology designed to detect and classify wireless threats, including rogue access points and other unauthorized activity.

Production data is not permitted to be used for test purposes in a non-production environment, unless equivalent security controls and need-to-know access apply, or the data is first masked or sanitized.

2.14 End-user computer and communication devices

J.B. Hunt takes the following measures to protect information stored on end-user computing devices:

Endpoints are protected from malware, spyware, and malicious attacks through daily on-access scans on programs and files along with malware signature updates deployed multiple times a day.

Only J.B. Hunt-authenticated devices may be connected to J.B. Hunt private networks. Visitors are permitted to connect to a guest network that is isolated from J.B. Hunt's private networks.

Emails routed in and out of Company mail servers are scanned and protected by our secure email relay.

Where technically feasible, J.B. Hunt remotely wipes the drives and other non-volatile memory of any individual computing devices that have been lost, stolen, or determined to be the target of malicious attempts to access or compromise the device.

Asset management processes are in place to identify, track and maintain Company-owned hardware, software, and IT infrastructure.

2.15 Third-party service providers

Third-party service providers may be required to enter into agreements with the Company that subject them to non-disclosure requirements, data protection, and security controls.

Before a third-party service provider is permitted to host or process data, J.B. Hunt conducts a thorough assessment of the service provider's security controls.

J.B. Hunt conducts security reviews on infrastructure managed by third parties to ensure that the provider adheres to Company security standards. Security reviews may include an annual review of certifications, penetration testing, and audit reports. The vendor management review and approval process for cloud service providers includes completion and review of a data protection and security questionnaire and related supporting documents.

2.16 Disruption resiliency and business continuity

Business units are responsible for defining, maintaining, and executing their continuity plans, with assistance and guidance provided by the Business Continuity Team.

J.B. Hunt's business continuity and disruption resiliency plans are designed to enable J.B. Hunt to continue its business operations following a natural or manmade disaster or other major event affecting J.B. Hunt operations, systems, and/or data. The following measures have been put in place to mitigate the effects of such events:

J.B. Hunt operates multiple geographically dispersed data centers with built-in redundancy and 24x7x365 on-site operations.

J.B. Hunt protects against loss of electrical power through an uninterruptible power supply and diesel generators.

Critical products hosted within data centers are designed to be highly redundant through the incorporation of advanced fault-tolerant features and components, such as server clustering, RAID storage, and multi-path connections.

Each data center is leveraged as a recovery site. If a major event impacts one facility, applications and services will be recovered to one of the remaining facilities. Automatic failover capabilities ensure that the entire infrastructure will be operational at the recovery site.

Data for critical applications is replicated across data centers on an on-going basis. Off-site backups are used to bring less-critical applications back online and are also a secondary resource for critical applications in the unlikely event that the replicated data is not available.

J.B. Hunt conducts business impact analyses on critical operations to identify potential disruptions and assess the impacts of those disruptions on business operations.

Business continuity plans are reviewed and tested on an annual basis.

Tests of failover and recovery mechanisms and procedures are conducted periodically.

2.17 Security incident management

J.B. Hunt's Cyber Security Incident Response Plan ("CSIRP") outlines a formal and coordinated approach for responding to cyber security incidents affecting data and information assets.

J.B. Hunt's Security Operations Center ("SOC") provides cyber defense and response services including threat intelligence fusion, threat detection and analysis, and incident response. The SOC manages identified security incidents and maintains records and a final report of such incidents in accordance with the CSIRP.

In the event of a cyber security incident, the SOC is authorized to engage the Cybersecurity Incident Response Team ("CSIRT") to address the response.

Security incidents are managed in accordance with documented incident response procedures and are reviewed by members of the CSIRT. Incidents are classified based on predefined criteria, including factors such as (a) the nature, date, and time of the incident; and (b) the affected information systems and any impacted confidential information.

After an initial review of an incident, the CSIRT coordinates with other Company functions, such as Legal, Privacy, and Human Resources, as appropriate to support investigation and response efforts.

Employees are required to report any known or suspected security incident.

In the event a security incident impacts customer-owned data, J.B. Hunt will notify the customer without undue delay and in accordance with any applicable customer agreement.

2.18 Data retention

J.B. Hunt maintains a records retention program designed to ensure that business records are managed in a structured, consistent manner across their lifecycle, from creation through disposition. Records are organized into defined classifications with retention schedules established based on applicable laws and regulations, as well as business and operational needs.

Retention policies require that records be retained for specified periods and then archived or deleted in accordance with those schedules. However, retention may be extended as necessary to comply with legal or regulatory obligations.

J.B. Hunt retains customer-owned data in accordance with the safeguards described in this document and the requirements of any applicable customer agreement.

2.19 Compliance with data privacy laws

J.B. Hunt's data privacy program is based on established data privacy principles and applicable legal frameworks.

When J.B. Hunt handles personal data, whether in connection with its workforce or the services it provides to its customers, it applies policies and procedures designed to ensure compliance with applicable data privacy laws and to guide the responsible handling of such information.

To the extent J.B. Hunt conducts any data transfers, the following technical, organizational, and contractual measures are applied:

a) Organizational measures: J.B. Hunt maintains policies and procedures to address privacy and data risk management issues, including data minimization, de-identification, confidentiality, data security, and data access requests.

b) Compliance with laws: J.B. Hunt complies with applicable data privacy laws and the terms of its agreements. With respect to customer data, J.B. Hunt has processes in place to notify the customer if it can no longer meet its obligations under any applicable law due to changes in the law or other circumstances.

c) Selling or sharing of confidential information: J.B. Hunt will not sell or share customer data, or otherwise transfer customer data to third parties, except as required by law or otherwise agreed with the customer.