



# Security Vulnerability Assessment Checklist

## Physical Security of Warehouses & Distribution Centers

Assess the physical security measures in place to protect assets and data within logistics facilities.

### Perimeter Fencing Condition

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor
- ☐ N/A

### Number of Security Cameras

### Camera System Coverage

- ☐ Full Perimeter
- ☐ Key Areas Only
- ☐ Limited Coverage
- ☐ None

### Access Control System Type (e.g., Keypad, Biometric)

- ☐ Keypad
- ☐ Biometric
- ☐ Card Reader
- ☐ Manual (Key)
- ☐ None

### Description of Warehouse Lighting Adequacy

Write something...

### Visitor Management Process

- ☐ Formal Log and Escort
- ☐ Sign-in Sheet
- ☐ Limited Oversight
- ☐ No Formal Process


### Number of Security Guards (if applicable)

Enter a number...

### Details about loading dock security measures (e.g., barriers, visibility)

Write something...

**Upload photos of perimeter security (e.g., fencing, gates)**

 Upload File

## Transportation Security

Evaluate security controls related to the physical transportation of goods, including vehicles and drivers.

### Vehicle Tracking System in Use?

- ☐ GPS Tracking
- ☐ RFID Tracking
- ☐ Manual Log
- ☐ None

### Security Measures in Vehicles?

- ☐ Alarm System
- ☐ Cameras (Interior/Exterior)
- ☐ Driver Background Checks
- ☐ Secure Compartments
- ☐ Vehicle Immobilizers
- ☐ Tamper-Evident Seals

### Number of Vehicles with Dash Cams?

Enter a number...

**Driver Training Program?**

- ☐ Yes, Comprehensive Program
- ☐ Yes, Basic Security Awareness
- ☐ No Formal Program

**Describe Vehicle Route Security Protocols**

Write something...

**Last Vehicle Security Audit Date**

Enter date...

**Primary Vehicle Dispatch Location**

 Set My Current Location



**Data Security & Privacy**

Review practices concerning the collection, storage, processing, and transmission of logistics-related data, ensuring privacy and confidentiality.

### Data Encryption at Rest

- ☐ Fully Encrypted
- ☐ Partially Encrypted
- ☐ Not Encrypted

### Data Encryption in Transit

- ☐ TLS 1.3 or higher
- ☐ TLS 1.2
- ☐ SSL or earlier
- ☐ No Encryption

### Data Retention Period (in days)

Enter a number...

### Data Access Control Policy

Write something...

### Sensitive Data Types Collected

- ☐ Customer Addresses
- ☐ Shipping Manifests
- ☐ Payment Information
- ☐ Inventory Levels
- ☐ Tracking IDs
- ☐ Employee Data

### Data Subject Access Request (DSAR) Process

- ☐ Formal process in place
- ☐ Informal process
- ☐ No process in place

### Data Breach Notification Plan

Write something...

### Last Data Privacy Policy Review Date

Enter date...

## Network & System Security

Analyze the security posture of networks and systems used for tracking, inventory management, and communication within the logistics operation.

### Number of Wireless Access Points (WAPs) in each warehouse

Enter a number...

### Firewall Type(s) in use (select all that apply)

- ☐ Next-Generation Firewall
- ☐ Traditional Firewall
- ☐ Web Application Firewall (WAF)
- ☐ Cloud-Based Firewall
- ☐ None

### Network Segmentation Implemented? (select all that apply)

- ☐ VLANs
- ☐ Microsegmentation
- ☐ Firewall Rules
- ☐ No Segmentation

### VPN Configuration for Remote Access

- ☐ Always On
- ☐ On-Demand
- ☐ Not Configured
- ☐ Other (Specify in Long Text)

### Description of Intrusion Detection/Prevention System (IDS/IPS) configuration, if applicable.

Write something...


### Patch Management Process for Servers and Network Devices

- ☐ Automated
- ☐ Manual
- ☐ None

### Last Network Vulnerability Scan Date

Enter date...

## Network Diagram (Optional)

 Upload File

# Application Security (Logistics Software)

Evaluate the security of software applications used for route optimization, warehouse management, and transportation tracking.

### Is the application using a secure coding framework?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

### Are input fields validated to prevent injection attacks?

- ☐ Yes
- ☐ No
- ☐ Partially

### Version of the Application

Enter a number...

### Does the application implement proper authentication and authorization?

- ☐ Yes
- ☐ No
- ☐ Partially



### **Describe authentication mechanisms used (e.g., MFA, SSO)**

Write something...

### **Application Security Scan Results**

 Upload File

### **Are dependencies regularly updated to address known vulnerabilities?**

- ☐ Yes
- ☐ No
- ☐ Semi-Regularly

### **Describe any identified vulnerabilities and remediation plans.**

Write something...

## **Personnel Security & Training**

Assess the security awareness and access controls for employees and contractors involved in logistics operations.

### **Background Checks Conducted?**

- ☐ Yes - Full Criminal History
- ☐ Yes - Limited Criminal History
- ☐ No
- ☐ Partial/Varying

### Number of Employees Receiving Security Awareness Training (Past 12 Months)

Enter a number...

### Security Awareness Training Frequency?

- ☐ Annually
- ☐ Semi-Annually
- ☐ Quarterly
- ☐ Monthly
- ☐ As Needed

### Briefly describe the content of the security awareness training.

Write something...

### Training Topics Covered (Select all that apply)

- ☐ Phishing Awareness
- ☐ Password Security
- ☐ Data Handling & Privacy
- ☐ Physical Security Procedures
- ☐ Supply Chain Security
- ☐ Incident Reporting
- ☐ Social Engineering
- ☐ Insider Threat Awareness

### Role-Based Access Controls Implemented?

- ☐ Yes - Fully Implemented
- ☐ Yes - Partially Implemented
- ☐ No

### Last Security Training Review Date

Enter date...

### Describe process for onboarding new contractors related to security requirements

Write something...

## Supply Chain Security

Examine security practices of vendors and partners within the logistics supply chain to identify potential vulnerabilities.


### Vendor Security Assessment Program Exists?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

### Describe the process for vendor risk assessment (frequency, criteria, etc.)

Write something...

### Upload Vendor Security Questionnaires/Reports

 Upload File

### Number of critical suppliers assessed in the last year

Enter a number...

### Which security standards do suppliers adhere to?

- ☐ ISO 27001
- ☐ SOC 2
- ☐ CSA STAR
- ☐ Other (Specify in Long Text)

### Is there a contractual requirement for security standards in vendor agreements?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

### Describe the process for ongoing vendor security monitoring

Write something...

## Incident Response & Disaster Recovery

Evaluate the preparedness and capabilities for responding to security incidents and recovering from disasters impacting logistics operations.

**Describe the current Incident Response Plan (IRP) for logistics-related security events.**

Write something...

**What is the Recovery Time Objective (RTO) for critical logistics systems (e.g., warehouse management system)?**

Enter a number...

**What is the Recovery Point Objective (RPO) for critical logistics data?**

Enter a number...

**Date of last Disaster Recovery Drill (for logistics operations).**

Enter date...

**Which potential disaster scenarios are included in the Disaster Recovery Plan? (Select all that apply)**

- ☐ Natural Disasters (e.g., flood, earthquake)
- ☐ Cyberattacks (e.g., ransomware)
- ☐ System Failures (hardware, software)
- ☐ Supply Chain Disruptions
- ☐ Human Error
- ☐ Internal Sabotage


**Who is the designated Incident Response Team Lead for logistics?**

- ☐ Name and Contact Info (to be populated)

**Describe the process for communicating security incidents to stakeholders (internal and external).**

Write something...

**Upload copy of Disaster Recovery Plan documentation (if available).**

 Upload File

## Regulatory & Compliance

Verify adherence to relevant laws, regulations, and industry standards related to logistics security.

**Is the company compliant with GDPR (if applicable)?**

- ☐ Yes
- ☐ No
- ☐ Not Applicable

**Is the company compliant with C-TPAT (if applicable)?**

- ☐ Yes
- ☐ No
- ☐ Not Applicable

**Is the company compliant with ISO 28000 (Supply Chain Security)?**

- ☐ Yes
- ☐ No
- ☐ Not Applicable

### Last Compliance Audit Date (General Logistics)

Enter date...


### Summary of Previous Compliance Audit Findings & Remediation Actions

Write something...

### Number of reported breaches related to regulatory non-compliance in the last year

Enter a number...

### Upload Relevant Compliance Documentation (e.g., audit reports, certifications)

 Upload File

### Does the company maintain records demonstrating compliance with transportation security regulations (e.g., TSA)?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

## IoT Device Security (e.g., Trackers, Sensors)

Assess the security of any Internet of Things (IoT) devices used in logistics for tracking and monitoring, including firmware updates and data transmission security.

### Device Firmware Update Process

- ☐ Automated & Regularly Scheduled
- ☐ Manual & On-Demand
- ☐ No Formal Process

### Number of Unpatched Devices

Enter a number...

### Data Transmission Security

- ☐ HTTPS/TLS Encryption
- ☐ VPN Tunnel
- ☐ No Encryption
- ☐ Proprietary Encryption

### Device Authentication Method

- ☐ Pre-shared Key
- ☐ Certificates
- ☐ Username/Password
- ☐ None

### Description of Device Access Controls

Write something...



### Device Physical Security

- ☐ Locked in secure location
- ☐ Easily accessible
- ☐ Location is monitored

### Device Configuration File



Upload File