



Public Transport Depot Cybersecurity & Network Vulnerability Audit 2026 Checklist

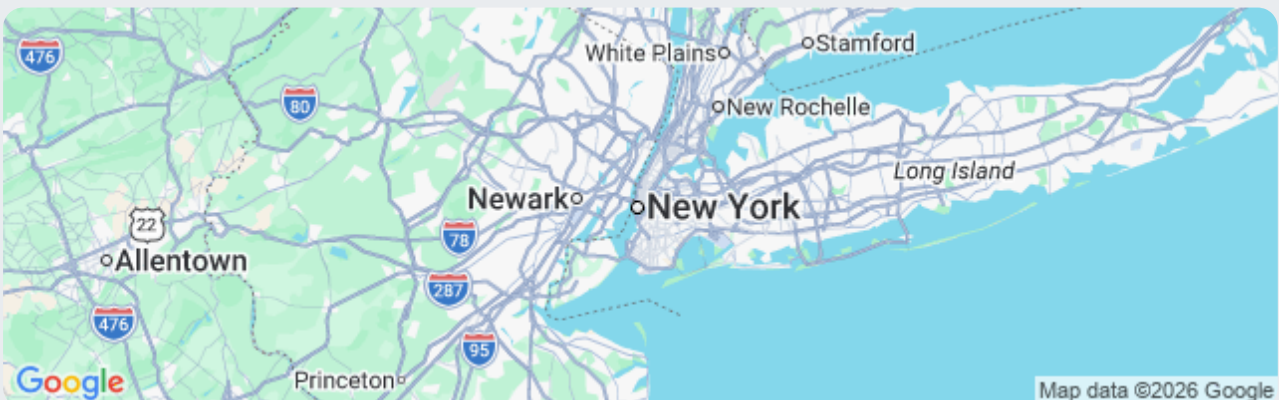
Network Infrastructure & Hardware Security

Assessment of physical and logical security for routers, switches, firewalls, and wireless access points within the depot environment.

Audit Inspection Date

Network Node/Server Room Location

 [Set My Current Location](#)



Hardware Assets Inspected

- ☐ Core Switches
- ☐ Edge Routers
- ☐ Firewall Appliances
- ☐ Wireless Access Points
- ☐ Network Storage (NAS/SAN)

Firewall Configuration Status

- ☐ Fully Compliant
- ☐ Minor Discrepancies
- ☐ Critical Vulnerabilities Found
- ☐ Not Applicable

Identified Network Vulnerabilities

Write something...

Network Topology Diagram/Evidence

 Upload File

Lead Network Auditor Signature

Access Control & Identity Management

Audit of user authentication protocols, multi-factor authentication (MFA) implementation, and management of privileged access rights.

Multi-Factor Authentication (MFA) Implementation Status

☐ Fully Implemented☐ Partially Imrolled☐ Not Implemented☐ N/A

Authorized Access Methods Verified

☐ Biometric Scanners☐ Smart Cards / RFID☐ Digital Certificates☐ Password-based Authentication☐ Hardware Tokens

Privileged Account Audit Date

Write something...

Identified Access Discrepancies or Unauthorized Account Findings

Write something...

User Access Review Log (Evidence)

 Upload File

Auditor Verification Signature

Endpoint Security & Device Management

Verification of security software, patch management, and anti-malware status for all depot workstations, tablets, and IoT-connected devices.

Device Type Identification

- ☐ Mobile Handheld/Tablet
- ☐ Desktop/Laptop Workstation
- ☐ IoT/Embedded Sensor
- ☐ On-Bus/On-Train Terminal

Antivirus/EDR Software Status

- ☐ Active & Up-to-date
- ☐ Active but Outdated
- ☐ Inactive/Not Installed
- ☐ Not Applicable

Last Security Patch Installation Date

Security Controls Verified

- ☐ Disk Encryption Enabled
- ☐ USB Ports Disabled/Restricted
- ☐ Automatic Screen Lock Active
- ☐ Unauthorized Software Scan Completed

Vulnerability Findings & Observations

Write something...

Endpoint Scan Report Upload

 Upload File

Auditor Verification Signature

Fleet Telematics & IoT Vulnerability Assessment

Review of the security layers protecting data transmission between vehicles, GPS units, and the central depot server.

Telematics Hardware Security Status

- ☐ Secure/Encrypted
- ☐ At Risk/Unencrypted
- ☐ Non-functional
- ☐ Unknown

Identified Vulnerabilities Found

- ☐ Unsecured Firmware
- ☐ Insecure Communication Protocol (e.g., Unencrypted MQTT)
- ☐ Default Credentials Still Active
- ☐ Unauthorized Device Connection
- ☐ No Software/Patch Updates Available

Number of IoT Devices Audited

Enter a number...

Detailed Vulnerability Findings

Write something...

Last Firmware Update Date

Enter date...

Upload Network Traffic Logs or Scan Reports

 Upload File

Data Encryption & Integrity Verification

Inspection of encryption standards for data at rest and data in transit, specifically for passenger data and operational logs.

Encryption Standard for Data at Rest

- ☐ AES-256
- ☐ AES-128
- ☐ RSA-2048
- ☐ Not Encrypted
- ☐ Other

Encryption Protocols in Use for Data in Transit

- ☐ TLS 1.3
- ☐ TLS 1.2
- ☐ SSL
- ☐ IPsec
- ☐ HTTPS

Last Data Integrity Audit Date

Enter date...

Encryption Key Management Procedure Summary

Write something...

Encryption Certificate Verification Report

 Upload File

Auditor Verification Signature

Network Monitoring & Intrusion Detection

Evaluation of the effectiveness of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and real-time logging capabilities.

Intrusion Detection System (IDS) Status

- ☐ Active and Monitoring
- ☐ Active but Alerts Silenced
- ☐ Inactive/Down
- ☐ Not Implemented

Monitored Network Segments

- ☐ Fleet Telematics Network
- ☐ Administrative/Office Network
- ☐ CCTV & Surveillance Network
- ☐ IoT & Sensor Network
- ☐ Public Wi-Fi/Guest Network

Recent Critical Security Alerts Summary

Write something...

Last System Log Review Date

Enter date...

Number of Unresolved High-Priority Alerts

Enter a number...

Upload Network Traffic Audit Report

 Upload File

Incident Response & Disaster Recovery Readiness

Testing of cybersecurity incident response plans, backup integrity, and the ability to restore critical transit operations after a breach.

Last Incident Response Plan Review Date

Enter date...

Incident Response Plan Status

- ☐ Active and Up-to-Date
- ☐ Requires Immediate Update
- ☐ Under Review
- ☐ Outdated/Expired

Verified Backup Types

- ☐ Off-site Cloud Backup
- ☐ On-premise Immutable Backup
- ☐ Physical Tape/Removable Media
- ☐ Real-time Data Mirroring

Summary of Last Disaster Recovery Drill Results

Write something...

Upload Latest Disaster Recovery Test Report

 Upload File

Auditor Verification Signature

Physical Security of IT Assets

Assessment of the physical protection of server rooms, network closets, and cabling against unauthorized physical tampering.

Server Room Access Status

- ☐ Fully Secured
- ☐ Unsecured / Door Ajar
- ☐ Security Lock Malfunction

Physical Security Measures Present

- ☐ CCTV Surveillance
- ☐ Biometric Access Control
- ☐ Security Guard Patrols
- ☐ Electronic Keycard System
- ☐ Motion Sensors

Observed Vulnerabilities or Unsecured Entry Points

Write something...

Photographic Evidence of Asset Security

 Upload File

Auditor Verification Signature



Employee Cybersecurity Awareness & Training

Audit of staff training records regarding phishing, social engineering, and secure handling of sensitive transport data.

Date of Last Security Awareness Training Session

Enter date...

Compliance Rate of Department Staff

- ☐ Below 75%
- ☐ 75% - 90%
- ☐ 91% - 100%

Training Topics Covered in 2026

- ☐ Phishing & Social Engineering
- ☐ Password Management & MFA
- ☐ Secure Remote Access
- ☐ Data Privacy & GDPR Compliance
- ☐ Physical Device Security

Training Attendance Logs & Certification Records

 **Upload File**

Summary of Identified Training Gaps or Personnel Risks

Write something...

Auditor Verification Signature



Third-Party Vendor & Supply Chain Risk Management

Review of security compliance for external contractors and software providers accessing the depot network.

Vendor Access Levels

- ☐ Full Network Access
- ☐ Remote Software Access Only
- ☐ Physical Depot Access Only
- ☐ No Direct Network Access

Last Security Compliance Audit Date

Enter date...

Vendor SOC2 or Security Certification Document

 Upload File

Vendor Risk Level

- ☐ Critical (High Risk)
- ☐ Medium (Moderate Risk)
- ☐ Low (Minimal Risk)

Summary of Identified Vendor Vulnerabilities

Write something...

Auditor Verification Signature

< Previous

> Next

✔ Finish

✎ Generate Sample Report