



Warehouse WMS Security Checklist

User Access & Authentication

Verify user access controls, password policies, and multi-factor authentication implementation.

Multi-Factor Authentication Enabled?

- ☐ Yes
- ☐ No
- ☐ Partial (some users)

Password Complexity Requirements?

- ☐ Strong (length, special characters)
- ☐ Medium
- ☐ Weak/None

Minimum Password Length (characters)

Last Password Policy Review Date

Privilege Escalation Controls?

- ☐ Strict – Requires Approval
- ☐ Limited – Self-service
- ☐ None

Describe User Access Review Process

Write something...

Role-Based Access Control (RBAC) Implemented?

- ☐ Yes
- ☐ No
- ☐ Partial

Data Encryption & Protection

Assess encryption methods for data at rest and in transit, and ensure proper key management procedures.

Encryption Method at Rest

- ☐ AES-256
- ☐ RSA
- ☐ Other (Specify in Long Text)

Specify Encryption Method (if 'Other' selected)

Write something...

Encryption Protocol for Data in Transit

- ☐ TLS 1.3
- ☐ TLS 1.2
- ☐ SSL 3.0 (Not Recommended)
- ☐ Other (Specify in Long Text)

Specify Encryption Protocol (if 'Other' selected)

Write something...

Key Length (in bits)

Enter a number...

Key Management Method

- ☐ Centralized Key Management System
- ☐ Hardware Security Module (HSM)
- ☐ Software-Based Key Management
- ☐ Other (Specify in Long Text)

Specify Key Management Method (if 'Other' selected)

Write something...

System Patching & Updates

Confirm timely application of security patches and software updates for the WMS and related infrastructure.

Last System Patch Applied Date

Enter date...

WMS Software Version Number

Enter a number...

Patching Method

- ☐ Automated
- ☐ Manual
- ☐ Hybrid

Next Scheduled Patching Date

Enter date...

Description of Patches Applied (Include Release Notes)

Write something...

Patching Server Status

- ☐ Active
- ☐ Inactive
- ☐ Maintenance

Network Security

Evaluate firewall configurations, intrusion detection/prevention systems, and network segmentation.

Firewall Type

- ☐ Hardware
- ☐ Software
- ☐ Cloud-based

Firewall Rule Count

Enter a number...

Intrusion Detection/Prevention System (IDS/IPS)

- ☐ Enabled
- ☐ Disabled
- ☐ N/A

Network Segmentation Description

Write something...

VPN Usage for Remote Access

- ☐ Enabled
- ☐ Disabled
- ☐ N/A

Last Network Vulnerability Scan Date

Enter date...

Data Backup & Recovery

Review backup schedules, storage locations, and disaster recovery procedures.

Last Successful Backup Timestamp (Epoch)

Enter a number...

Last Full Backup Date

Enter date...

Next Scheduled Full Backup Date

Enter date...

Backup Storage Location

- ☐ On-site
- ☐ Off-site (Cloud)
- ☐ Hybrid

Backup Retention Period (Days)

Enter a number...

Description of Disaster Recovery Plan

Write something...

Backup Type

- ☐ Full
- ☐ Differential
- ☐ Incremental

Recovery Time Objective (RTO) - Hours

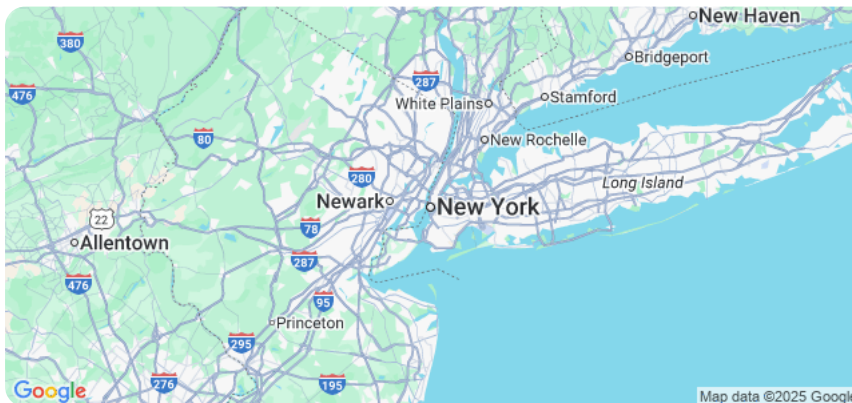
Enter a number...

Physical Security

Assess physical access controls to WMS servers and data storage facilities.

Server Room Location

[Set My Current Location](#)



Access Control Methods Implemented

- ☐ Keycard Access
- ☐ Biometric Scan
- ☐ Security Guard
- ☐ PIN Code

Number of Security Cameras

Enter a number...

Visitor Policy

- ☐ Mandatory Sign-In
- ☐ Escorted Visits Only
- ☐ No Visitor Access

Last Physical Security Audit Date

Enter date...

Details of Physical Security Measures (e.g., perimeter fencing, lighting)

Write something...

Audit Trails & Logging

Validate the existence and integrity of audit trails to track user activities and system events.

Number of Audit Log Files Rotated Per Month

Enter a number...

Last Audit Log Review Date

Enter date...

Summary of Audit Log Review Findings

Write something...

Audit Log Retention Policy Compliance

- ☐ Compliant
- ☐ Non-Compliant
- ☐ N/A

Logged Events (Select all that apply)

- ☐ User Logins
- ☐ Data Modifications
- ☐ System Configuration Changes
- ☐ Report Generation
- ☐ Inventory Adjustments

Frequency of Real-Time Log Monitoring

Enter time...

Vendor Security Assessment

Review security practices and certifications of the WMS vendor.


Vendor Security Policy Summary

Write something...

Vendor Security Certification(s)

- ☐ ISO 27001
- ☐ SOC 2
- ☐ PCI DSS
- ☐ Other (Specify)

Vendor Security Assessment Report

 Upload File

Date of Last Vendor Security Assessment

Enter a number...

Vendor Vulnerability Management Process

- ☐ Formal Program
- ☐ Informal Process
- ☐ No Defined Process

Incident Response Plan

Assess the existence and effectiveness of the incident response plan for security breaches.

Summary of Incident Response Plan

Write something...

Incident Severity Levels Defined?

- ☐ Yes
- ☐ No
- ☐ Not Applicable

Estimated Time to Contain Incident (Hours)

Enter a number...

Date of Last Incident Response Plan Review

Enter date...

Communication Channels Used During Incident?

- ☐ Email
- ☐ Phone
- ☐ Instant Messaging
- ☐ Dedicated Incident Management Platform

Roles & Responsibilities Clearly Defined?

- ☐ Yes
- ☐ No
- ☐ Partially Defined

Compliance & Regulations

Verify adherence to relevant security standards and industry regulations (e.g., GDPR, PCI DSS).

Relevant Compliance Standards?

- ☐ GDPR
- ☐ PCI DSS
- ☐ CCPA
- ☐ ISO 27001
- ☐ Other

Specific Compliance Requirements?

Write something...

Last Compliance Audit Date

Enter date...

Data Sensitivity Level (1-5)

Enter a number...

Applicable Data Privacy Principles

- ☐ Data Minimization
- ☐ Purpose Limitation
- ☐ Storage Limitation
- ☐ Accuracy
- ☐ Integrity and Confidentiality

Regulatory Contact Name

Write something...