Mirazon
Providing Vision for Technology Solutions

Cybersecurity & Compliance Checklist for MWL Operations

Protect your production. Safeguard your data. Stay compliant.

Manufacturing, warehousing, and logistics (MWL) businesses rely on a unique mix of modern IT systems, industrial control systems (ICS), and sometimes decades-old equipment. That blend is what keeps your operations running—but it's also what makes you an attractive target for cyberattacks.

Use this checklist to identify gaps, strengthen your defenses, and keep your operations compliant and resilient.

#1 Secure Your Network & Infrastructure

- [ ] Segment IT networks so production systems are separate from business systems.
- [ ] Update firewalls and intrusion detection/prevention systems with the latest patches and threat rules.
- [ ] Turn on multi-factor authentication (MFA) for all critical systems and remote access points.
- [ ] Use secure VPNs for all vendor or remote technician connections.

#2 Manage Legacy Systems & Outdated Technology

- [ ] Create an inventory of all legacy systems (e.g., Windows 95, XP, Windows Server 2008, etc.).
- [ ] Disconnect outdated machines from the internet and unnecessary network connections.
- [ ] Put compensating controls in place (application whitelisting, strict permissions, continuous monitoring).
- [ ] Build a lifecycle plan to upgrade or securely integrate outdated equipment.

#3 Control Access & Identities

- [ ] Give users only the minimum access they need (least privilege).
- [ ] Review user accounts regularly and remove inactive or unnecessary ones.
- [ ] Enforce strong password rules and rotate passwords on a set schedule.

PRO TIP: This includes end users with administrative access or rights.

#4 Protect and Back Up Your Data

- [ ] Back up all critical business and production data on a regular schedule.
- [ ] Store at least one backup offline or in air-gapped/immutable storage to block ransomware.
- [ ] At least once every quarter, verify that you can restore your data from backups.

#5 Prepare for Incidents

- [ ] Write (or update) your incident response plan with MWL operations in mind.
- [ ] Run tabletop exercises to rehearse the plan with your IT and operations staff.
- [ ] Keep a current contact list of key vendors and emergency support partners.

#6 Train and Remind Your Team

- [ ] Hold recurring cybersecurity training with real-world manufacturing threat examples.
- [ ] Send simulated phishing tests to measure readiness.
- [ ] Post quick security reminders in production areas, break rooms, and common spaces.

#7 Stay Compliant

- [ ] Identify which regulations apply to you (NIST, ISO 27001, CMMC, etc.).
- [ ] Schedule periodic compliance audits to catch and fix gaps early.
- [ ] Keep your cybersecurity policies documented and review them at least yearly.

PRO TIP: Legacy equipment doesn't have to be your biggest risk. Isolate it, monitor it, and secure it until you're ready for an upgrade.

Don't wait for a cyber incident to disrupt production.

We help manufacturing, warehousing, and logistics operations lock down vulnerabilities, protect legacy systems, and meet compliance standards—without slowing you down.

Contact us today to get started!

Mirazon®

Contact Us