MANUFACTURING

Industrial IT Strategy Guide

Keep the line running and the plant floor protected from office-side threats.

Manufacturers run office IT and plant-floor technology side by side, often on the same network. Downtime is measured in lost production, and defense suppliers face CMMC requirements. This guide covers how to connect the two worlds safely.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Plant floor and operations

- [ ] **Production systems (OT) separated from office IT**
  Ransomware that hits email should not reach the line.
- [ ] **Inventory of every machine, controller, and connected device**
  You cannot protect what you have not listed.
- [ ] **ERP and MES integrated and backed up**
  Orders, scheduling, and quality data in one place.
- [ ] **Reliable plant-floor Wi-Fi and wired network**
  Scanners and terminals need coverage everywhere.
- [ ] **Secure vendor remote access, logged and time-limited**
  Machine vendors should not have always-on access.

02 Security and compliance

- [ ] **Multi-factor authentication on email, ERP, and remote access**
  Stolen credentials start most incidents.
- [ ] **Endpoint protection monitored 24/7 on office systems**
  And documented exceptions for OT systems that cannot run it.
- [ ] **CMMC and NIST 800-171 readiness if you supply defense contracts**
  Know your level and your gaps.
- [ ] **Patch plan for systems that cannot be updated during production**
  Scheduled windows, tested first.
- [ ] **Security awareness training for office and floor supervisors**
  Phishing reaches everyone with an email address.

03 Resilience and growth

- [ ] **Backups of ERP, CAD, and machine programs with off-site copies**
  Machine programs are often stored in one place.
- [ ] **Recovery time targets for each critical system**
  Know what an hour of downtime costs.
- [ ] **Hurricane plan for equipment, data, and restart**
  Gulf Coast plants need a restart checklist.
- [ ] **Lifecycle plan for aging PCs that run machines**
  Plan replacements before failures stop a line.
- [ ] **Quarterly IT review tied to production plans**
  New lines need network and IT planning.

Red flags we see most

- Office and plant floor share one flat network.
- Machine vendors have permanent remote access.
- CNC programs live on one PC with no backup.
- Nobody knows the cost of an hour of downtime.

Where to start

Separate the plant floor network from the office first. It is the single best protection against an office-side ransomware attack stopping production.

Want a second set of eyes?

Book a free 30-minute IT assessment. A senior technician walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a free assessment

(813) 999-0086
swfit.io/free-consultation