

The Manufacturer's Cybersecurity & Compliance Checklist for 2026

A 12-Point Guide to Securing Your Idaho Manufacturing Business & Meeting Key Cyber Standards

Protect your business. Stay compliant. Win more contracts.

Built specifically for Idaho-based manufacturers navigating cybersecurity threats and regulatory frameworks.

Presented by:



Tr todyl

Idaho's Trusted Cybersecurity & Compliance Partner

Modular, Best-In-Class Security Capabilities Consolidated Into A Single Platform



Quick Self-Test: Are You at Risk? Check all that apply:

We use legacy or unsupported software in our production or back office
We store or transmit customer, vendor, or sensitive internal data
We don't conduct regular cybersecurity awareness training
We have no documented cybersecurity incident response plan
We are unsure if we are compliant with frameworks like NIST or CMMC

If you checked even one box, your business is exposed to cybersecurity risk — and may be out of compliance.

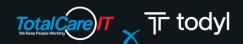




12-Point Cybersecurity Readiness Checklist Use this to assess where your cybersecurity posture stands today:

Cybersecurity Best Practice

	Multi-factor authentication (MFA) is enabled on all systems
	Endpoint protection and antivirus are deployed and monitored
	Backups are tested regularly and stored off-site
	Firewalls and network segmentation are in place
	Access to systems is based on roles/least privilege
	Regular patching and updates are scheduled and documented
	Employees complete annual cybersecurity awareness training
	Incident response plan exists and has been tested
	Vendor and supply chain risks are assessed regularly
	Remote access is secured with VPN or Zero Trust practices
	Admin privileges are tightly controlled and audited
П	An IT partner monitors and audits cybersecurity systems proactively





What You Need to Know About Compliance

If you're part of a defense supply chain, handle sensitive customer data, or want to win large contracts, you'll likely need to comply with:

CMMC 2.0 (Cybersecurity Maturity Model Certification)

A Department of Defense (DoD) requirement that mandates specific cybersecurity controls depending on your contract level.

NIST SP 800-171

A foundational framework that outlines best practices and safeguards for protecting controlled unclassified information (CUI).

Many Idaho manufacturers aren't fully compliant — and don't know it.

Compliance isn't optional — it's your gateway to contracts, credibility, and operational resilience.



Powered by TotalCareIT.net Cybersecurity & Compliance Experts for Idaho Manufacturers

Want help evaluating your risk profile? Visit our website or book a consultation.

Contact us today to learn how we can help.

TotalCare IT has offices in Boise, ID and Idaho Falls, ID. This allows us to effectively serve Western Idaho and Eastern Idaho.

428 Park Ave, Idaho Falls, ID 83402

5519 N Glenwood St, STE 130, Garden City, ID 83714

- (208) 881-9713 Sales
- (208) 881-0304 Current Clients
- info [at] totalcareit.net