42 Easy, Powerful Ways to Rapidly Enhance Your Cybersecurity

NORTEC®

It's time to simplify cybersecurity. This checklist takes the standards you use to keep your home safe and applies them to your organization's digital and physical assets. Follow each step and create a cybersecure business.

Create a Floorplan

□ **1.** Inventory all assets (hardware, networking, connectivity)

□ **2.** Maintain service and data catalogs

□ **3.** Know what data you have, where it's kept and how it's processed

□ **4.** Classify data based on industry standards and compliance requirements (e.g., general, confidential, MnA legal, company secret, PII)

Lock and Deadbolt the Door

□ **5.** Require passwords on all accounts, including cloud storage, backup systems and data sharing

□ **6.** Prevent access from geographies where you don't operate

□ **7.** Set up conditional access policies and multifactor authentication

□ **8.** Block legacy authentication methods that do not support multifactor authentication (e.g., POP3, IMAP)

Don’t Give Everyone a Key

□ **9.** Only allow authorized users and devices to access your information systems

□ **10.** Establish separate administrative and user accounts

□ **11.** Adhere to the principle of least privilege — limit rights based on what’s required to work

□ **12.** Give administrators separate accounts for user level and administrative tasks

□ **13.** Keep unauthorized individuals out of server and network equipment locations

Close the Back Door

□ **14.** Prevent criminals from using external systems and guest Wi-Fi to sneak into your network

□ **15.** Train users as to appropriate use of external systems

□ **16.** Limit access to external systems by application

□ **17.** Use controls (like Microsoft Cloud App Security) to discover and sanction access to online applications and services, implement application controls in firewalls or both

□ **18.** Prevent company devices from joining guest Wi-Fi networks

Want to get more government contracts?

Contact Nortec. We’ll help you prepare for your CMMC Audit.

BOOK A CONSULTATION

Know Who’s Visiting – And Watch Them

□ **19.** Establish controls so you can pinpoint activity to a specific user, device or visitor

□ **20.** Do not permit anonymous access, shared accounts, default passwords

□ **21.** Validate access using MFA and conditional access

□ **22.** Revalidate when unusual or risky activity is detected

□ **23.** Manage building, server room and equipment location keys/keycards

□ **24.** Log digital and physical access to systems and information

□ **25.** Retain and audit records

□ **26.** Review physical access at least once a year

□ **27.** Gain visibility, reporting and control over devices with tools like Defender for Endpoint

□ **28.** Escort guests and monitor their activity

Keep Out Nosy Neighbors

□ **29.** Use firewalls and “Always On” VPN to control communications on company devices

□ **30.** Don’t let people reach your internal systems directly from the internet

□ **31.** Separate public-facing services from internal production systems through cloud and hosting services or a DMZ network

Clean and Renovate

□ **32.** Delete data and applications before devices leave your possession — wipe or physically destroy USBs, external drives, backup media, CDs, DVDs and printers

□ **33.** Use vendor-supported systems and applications

□ **34.** Retire unsupported systems and applications

□ **35.** Turn on automated updates to automatically get the latest security fixes

□ **36.** Monitor, report and remediate vulnerabilities on servers and endpoints with device management apps

Get a Security System

Protect your organization with in-depth defense

□ **37.** Add advanced threat protection to Microsoft Exchange, SharePoint, OneDrive and Teams

□ **38.** Put Defender for Endpoint on workstations and servers

□ **39.** Continually scan for malware

□ **40.** Install a firewall

□ **41.** Update antivirus and endpoint protections with the latest malicious codes and threats

□ **42.** Scan for threats delivered before an update occurred

Not confident in DIY security?

We can assess your security and help you protect your organization. Start here.

GET A SECURITY ASSESSMENT NOW