GLOBALTSS
TECHNOLOGY SALES AND SERVICES // MARQUETTE, MI

# UP Business Cybersecurity Checklist

A practical self-audit covering the security basics every Upper Peninsula business should have in place. Check off each item honestly — this is meant to find real gaps, not make you feel good.

## 01 // ACCESS & AUTHENTICATION

- [ ] Multi-factor authentication (MFA) is enabled on all email accounts

  *Email is the #1 entry point for attackers. MFA stops most account takeovers cold.*

- [ ] MFA is enabled on all remote access and admin accounts

  *Remote desktop and VPN access without MFA is a common ransomware entry point.*

- [ ] Default passwords have been changed on all routers, firewalls, and devices

  *Default credentials are publicly documented online for most hardware models.*

- [ ] Former employees' accounts are disabled within 24 hours of departure

  *Lingering access for departed staff is an overlooked but serious risk.*

## 02 // BACKUP & RECOVERY

- [ ] Backups run automatically without manual action required

  *Manual backup processes get skipped. Automation removes human error.*

- [ ] At least one backup copy is isolated from your main network

  *Ransomware that reaches your backups defeats the purpose of having them.*

- [ ] Backups have been test-restored in the last 90 days

  *An untested backup is a guess, not a guarantee.*

- [ ] You know exactly how long a full restore would take

  *Recovery time matters as much as recovery possibility during an actual incident.*

## 03 // ENDPOINT & NETWORK SECURITY

- [ ] All computers have active, monitored endpoint protection (not just free antivirus)

  *Monitored detection catches threats that passive antivirus misses.*

- [ ] All software and operating systems are set to auto-update or are patched monthly

  *Unpatched systems have publicly known vulnerabilities attackers actively scan for.*

- [ ] Guest Wi-Fi is on a separate network from business systems

  *An unsegmented network lets a compromised guest device reach everything else.*

- [ ] A firewall is in place and its rules have been reviewed in the last year

  *Firewalls configured years ago often have outdated, overly permissive rules.*

## 04 // PEOPLE & PROCESS

- [ ] Staff have received phishing awareness training in the last 12 months

  *Most successful attacks start with one employee clicking the wrong link.*

- [ ] There is a written policy for handling suspicious emails

  *Staff need to know exactly who to contact when something looks off.*

- [ ] You have a written incident response plan for a security event

  *Confusion in the first hour of an incident usually makes the damage worse.*

- [ ] Someone other than you knows your IT systems well enough to respond in an emergency

  *Single points of failure include people, not just servers.*

## 05 // COMPLIANCE & INSURANCE

- [ ] You know which compliance frameworks (if any) apply to your business

  *HIPAA, PCI-DSS, CMMC, and others apply more broadly than most owners realize.*

- [ ] Your cyber insurance policy's security requirements are documented and met

  *Insurers increasingly deny claims when required controls were not actually in place.*

- [ ] Vendor agreements with access to your data include security requirements

  *A vendor breach is still your liability if there is no documented oversight.*

## // HOW TO SCORE YOURSELF

**18-19 checked:** Strong security posture. Keep maintaining it — controls decay without upkeep.
**13-17 checked:** Reasonable foundation with real gaps. These are fixable, usually quickly.
**Under 13 checked:** Meaningful exposure. This does not mean disaster — it means clear, specific next steps.

// WANT A PROFESSIONAL REVIEW?

**Get a free 30-minute IT assessment from GlobalTSS LLC.**
No obligation, no sales pitch — just an honest look at where you stand. Call or text (906) 662-4481 or visit globaltss.com/assessment