

20 Critical IT Responsibilities

for your small to mid-sized accounting firm

Whether You're In-House,
Outsourced, or Still Doing It Yourself

nimbl

TECH



Why This Checklist Matters

Phishing attacks are getting more sophisticated. Sensitive client data is at greater risk. And without a reliable IT helpdesk, your internal teams lose hours, sometimes days, trying to fix avoidable issues.

Most accounting firms are doing some of the right things. But few are doing all of them. This list is your baseline. Use it to close the gaps, reduce time-wasting tech issues, and improve cybersecurity before it impacts your clients or compliance.

Here are 20 foundational responsibilities every IT provider, MSP, or internal team should cover.

It's your checklist to get secure and stay that way.



Tools & Technology

01

Implement a Password Manager Firm-Wide

- ✓ Centralize credentials and reduce password reuse.
- ✓ **We recommend:** 1Password for ease of use and admin features.
- ✓ **Top picks:** 1Password, Bitwarden, Keeper

02

Require Multi-Factor Authentication (MFA) Everywhere

- ✓ Adds protection even if passwords are compromised.
- ✓ **Tip:** 1Password can double as an authenticator app.

03

Deploy Antivirus & Anti-Malware Across All Devices

- ✓ Protects in real-time from ransomware and keyloggers.
- ✓ **We recommend:** Malwarebytes
- ✓ **Top picks:** SentinelOne, CrowdStrike, Malwarebytes

04

Use a VPN When on Public Wi-Fi

- ✓ Encrypts traffic to prevent eavesdropping.
- ✓ **We recommend:** Harmony SASE
- ✓ **Top picks:** NordLayer, Harmony SASE, Cisco AnyConnect

05

Restrict Use of Flash Drives and External Media

- ✓ Prevents malware, data loss, and corruption.
- ✓ **We recommend:** Malwarebytes

06

Enable Remote Lock/Wipe Capabilities

- ✓ Protects lost or stolen devices.
- ✓ **We recommend:** DriveStrike for simplicity
- ✓ **Top picks:** Jamf, DriveStrike, JumpCloud

07

Block High-Risk and Non-Work Websites

- ✓ Reduces malware exposure and workplace distractions.

08

Implement Device Management (MDM)

- ✓ Centrally manage laptops, tablets, and phones.
- ✓ **We recommend:** Jamf
- ✓ **Popular options:** Microsoft Intune, Jamf, Kandji

09

Manage Google Workspace or Microsoft 365 Securely

- ✓ Configure permissions, email security, and access policies.
- ✓ **Tip:** Google Admin and Microsoft Entra require custom setup, not just out-of-the-box use.

10

Keep All Software and Operating Systems Updated

- ✓ Automate updates to close vulnerabilities.
- ✓ **Remember:** Many MDMs can automate this for you.



Security Policies & Best Practices

11

Maintain a Written Information Security Plan (WISP)

- ✓ Required by FTC (for accounting firms) and IRS (for tax preparers).

15

Audit Internal Access & Client Access Periodically

- ✓ Prevent privilege creep and over-permissioning.

12

Have a Business Continuity & Disaster Recovery Plan

- ✓ Protects against outages and ransomware. Helps with cyber insurance qualification.

16

Limit Access to Sensitive Data (Least Privilege)

- ✓ Only allow access to data needed for each person's role.

13

Conduct Regular Cybersecurity Training

- ✓ Educate your team, their behavior is your biggest risk.
- ✓ **We recommend:** HookSecurity
- ✓ **Popular options:** KnowBe4, PhinSec, HookSecurity

17

Appoint Someone Accountable for IT & Security

- ✓ Whether outsourced or not, someone must own it.

14

Run Internal Phishing Simulations

- ✓ Train your team to detect modern phishing threats.
- ✓ **We recommend:** Nimbl Tech, the only accounting-specific phishing simulator (QBO, Gusto, Bill, etc.)



Strategic Operations & Future-Proofing

18

Review Third-Party Vendor Risks

- ✓ Confirm SOC 2 Type II compliance, ask how they protect your data.

20

Evaluate Emerging Tools Like AI

- ✓ Use tools like ChatGPT to boost efficiency, but never input any sensitive information into models that learn from user data.
- ✓ **Tip:** Always check how AI tools handle your data before use.

19

Secure Email with SPF, DKIM & DMARC

- ✓ Prevent spoofing and phishing from your domain.

Final Thoughts

You don't need to tackle all 20 items at once, but each one matters. If you're a growing firm, or already outsourcing your IT, use this checklist to prioritize, evaluate your provider, and confidently scale.



Let's talk about how Nimbl Tech can help you put this checklist into action.

[Let's Talk Tech](#)

nimbl

TECH

Fractional IT for remote teams

[Explore Nimbl Tech](#)