CPA Cybersecurity Checklist

24 practical security checks across 7 critical areas | Curetopia Networks

Mark each item complete, in progress, or needing attention. Assign an owner and target date to gaps.

Identity & access

- ■ Require MFA for Microsoft 365, Google Workspace, remote access, and administrator accounts.
- ■ Use separate administrator accounts and least-privilege access.
- ■ Review terminated employees, shared accounts, guest users, and stale access quarterly.

Endpoint & network security

- ■ Deploy centrally managed endpoint protection and timely security patches.
- ■ Encrypt laptops and require screen locks; document lost-device response.
- ■ Segment guest Wi-Fi from business systems and protect remote access.

Client data & tax applications

- ■ Limit access to taxpayer data based on job responsibilities.
- ■ Protect tax/accounting application data, reports, and exports.
- ■ Use approved secure portals for sharing sensitive documents.

Backup & recovery

- ■ Maintain encrypted, isolated or immutable backups of critical files and systems.
- ■ Define recovery time and recovery point objectives for tax-season operations.
- ■ Test restoration and document who can initiate recovery.

Email & fraud prevention

- ■ Configure SPF, DKIM, and DMARC with monitoring and an enforcement plan.
- ■ Train staff to verify payment, banking, and client-detail changes out of band.
- ■ Provide a phishing-reporting and suspicious-email escalation process.

Policies, vendors & incident response

- ■ Maintain a written information security plan (WISP) and assign an accountable owner.
- ■ Review applicable IRS Publication 4557, FTC Safeguards Rule, and state requirements with counsel.
- ■ Document vendor access, incident reporting, notification escalation, and security reviews.

AI security & taxpayer data protection

- Adopt a written employee policy for permitted AI uses and prohibited data inputs.
- Do not enter confidential taxpayer information into unapproved public AI tools.
- Assess approved AI vendors for retention, training use, confidentiality, and data sharing.
- Apply enterprise access controls and contractual safeguards to approved AI services.
- Train staff to recognize AI-related confidentiality and disclosure risks.
- Independently verify AI-generated tax research, citations, calculations, and advice.

IRS guidance on AI: The IRS Office of Professional Responsibility discusses public/unsecured AI disclosure risks and professional duties in *Introductory Guidelines for Responsible AI Use in Federal Tax Practice* (2026).

Source: https://www.irs.gov/pub/opr-taxpros/issue-number-2026-19-introductory-guidelines-for-responsible-ai-use-in-federal-tax-practice.pdf

Legal context: IRC sections 6713 and 7216 address unauthorized use or disclosure of tax return information by preparers. AI use is not automatically a violation; requirements and penalties depend on the facts.

Curetopia Networks Inc. | curetopianetworks.com | 317-820-2105

Educational only; not a certification, audit, legal opinion, or guarantee of compliance. Consult qualified legal and tax compliance advisers.