FTC Safeguards Expanded Compliance Guide

For CPA Firms and Tax Professionals

This expanded guide explains each requirement in the FTC Safeguards Rule.
Use the Yes/No checkboxes to assess your firm's current compliance level.

1. Governance and Security Leadership

Yes: ☐ No: ☐ We have a designated qualified person responsible for our security program.
Explanation: The FTC requires every firm to appoint a person who oversees cybersecurity policies and program development.

Yes: ☐ No: ☐ We review our security program at least once per year.
Explanation: Annual reviews help ensure your program remains aligned with new risks, staffing changes, and technology updates.

Yes: ☐ No: ☐ We have written policies for data handling, access control, and security expectations.
Explanation: Written documentation is required and forms the foundation of staff accountability and regulatory readiness.

2. Risk Assessment

Yes: ☐ No: ☐ We have completed a formal risk assessment in the past 12 months.
Explanation: Risk assessments identify vulnerabilities in systems, vendors, processes, and staff behaviors.

Yes: ☐ No: ☐ Our assessment identifies both internal and external risks to client data.
Explanation: Regulations require identifying risks from insiders, cyberattacks, vendors, and technology failures.

Yes: ☐ No: ☐ We have documented mitigation steps for each identified risk.
Explanation: A risk register or mitigation plan is required to demonstrate ongoing improvement.

3. Access Controls

Yes: ☐ No: ☐ All user accounts require strong, complex passwords.
Explanation: Weak passwords are the most common cause of account compromise.

Yes: ☐ No: ☐ Multifactor authentication (MFA) is enabled for all staff.
Explanation: MFA is required for any system storing or accessing customer financial information.

Yes: ☐ No: ☐ We limit access to client data to only essential personnel.
Explanation: Least-privilege access reduces exposure and limits the blast radius of an incident.

FTC Safeguards Expanded Compliance Guide (Continued)

4. Encryption

Yes: ☐ No: ☐ Client data is encrypted at rest on all devices.
Explanation: Encryption ensures data remains protected even if a device is stolen or accessed improperly.

Yes: ☐ No: ☐ Client data is encrypted in transit.
Explanation: Data must be encrypted when transmitted over networks, email, or remote connections.

5. Secure Data Storage and Disposal

Yes: ☐ No: ☐ We securely store all sensitive client records.
Explanation: Only authorized personnel should have access to stored financial information.

Yes: ☐ No: ☐ We have a formal retention and destruction policy.
Explanation: Policies should define how long data is kept and how it must be destroyed.

Yes: ☐ No: ☐ We securely dispose of old files, devices, and backups.
Explanation: Data-bearing devices must be shredded or securely wiped.

6. Monitoring and Threat Detection

Yes: ☐ No: ☐ We use antivirus or EDR on all workstations and servers.
Explanation: EDR provides real-time threat detection and is now standard for compliance.

Yes: ☐ No: ☐ We actively monitor for suspicious activity.
Explanation: Continuous monitoring ensures anomalies are detected quickly.

Yes: ☐ No: ☐ We receive alerts when security issues occur.
Explanation: Alerts reduce response time and minimize business impact.

7. Vendor Management

Yes: ☐ No: ☐ We maintain a list of all vendors who handle or store client data.
Explanation: Vendor inventory is required to evaluate third-party risk.

Yes: ☐ No: ☐ We verify the security of each vendor.
Explanation: Due diligence helps ensure vendors maintain acceptable safeguards.

Yes: ☐ No: ☐ We have signed agreements defining security responsibilities.
Explanation: Contracts must spell out roles, expectations, and incident reporting obligations.

FTC Safeguards Expanded Compliance Guide (Continued)

8. Employee Security Training

Yes: ☐ No: ☐ All staff receive security awareness training at least once per year.
Explanation: Employees must understand phishing, password hygiene, and data handling requirements.

Yes: ☐ No: ☐ We conduct phishing simulations or similar tests.
Explanation: Simulations reinforce training and help measure risk exposure.

Yes: ☐ No: ☐ We follow documented onboarding and offboarding procedures.
Explanation: Account creation and removal must follow strict processes.

9. Incident Response

Yes: ☐ No: ☐ We have a documented incident response plan.
Explanation: A written plan defines immediate steps, communication paths, and escalation processes.

Yes: ☐ No: ☐ Staff know who to contact during an incident.
Explanation: Clear instructions reduce confusion under pressure.

Yes: ☐ No: ☐ We retain logs needed for investigations.
Explanation: Logs allow forensic investigation and support insurance claims and reporting obligations.

FREE Personalized Safeguards Review

If your checklist revealed any No answers, or if you want help interpreting your results, we offer a free, no■obligation Safeguards Review for CPA firms and tax professionals.

During your session, you will receive:
• A prioritized list of risks based on your answers
• Guidance on what the FTC expects from firms of your size
• Specific remediation steps you can take immediately
• Answers to questions about insurance, compliance, and documentation

To schedule your free review, contact us today:
Email: support@asteroidit.com
Phone: 480■771■9871

Your clients trust you with their most sensitive data, and you can trust us to help you protect it.