



9 ELEMENTS OF FTC SAFEGUARDS SECURITY PROGRAM

The FTC Safeguards Rule outlines 9 separate components required for compliance. Each section listed below is a brief description of the core idea for each element followed by a direct link to the actual standard.

1 DESIGNATE A QUALIFIED INDIVIDUAL

- In charge of overseeing/implementing the information security program
- Can be an employee, affiliate, or service provider of the client
- Client retains responsibility if delegated outside their organization
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(a\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(a))

2 PERFORM AND DOCUMENT RISK ASSESSMENT

- Must be a written assessment
- Must include criteria for evaluating risks and assessment of systems and customer information
- Requires a continuing cadence for additional assessments
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(b\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(b))

3 APPLY CONTROLS

- Implement and periodically review access controls
- Deploy encryption for customer data in transit and at rest
- Annual penetration tests
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(c\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c))

4 VALIDATE CONTROLS

- Regularly test and monitor controls' effectiveness
- Information systems require continuous monitoring or annual penetration testing
- Vulnerability assessments every six months
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(d\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(d))

5 DEVELOP TRAINING/AUDITING PROGRAM

- Implement security awareness training explaining risk assessment findings
- Maintain sufficient staffing to run the security program
- Verify that security personnel are staying current on security threats
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(e\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(e))

6 MONITOR SERVICE PROVIDERS

- Engage service providers that can maintain appropriate safeguards
- Make sure service provider contracts include safeguard implementation
- Periodically assess service providers
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(f\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(f))

7 DEVELOP CONTINUOUS IMPROVEMENT CADENCE

- Evaluate information security program based on:
 - Testing
 - Material changes in your organization
 - The results of a risk assessment
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(g\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(g))

8 DOCUMENT INCIDENT RESPONSE PLAN

- Document every incident
- Include goals, processes, and roles among several other requirements
- Review response plan after every security event
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(h\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(h))

9 PROVIDE ANNUAL REPORTING TO SENIOR LEADERSHIP

- Designated Qualified Individual must provide annual report to leadership body
- Include overall status of security program and compliance
- Must also have material matters related to the information security program (assessments, incident reports, improvement recommendations, etc.)
- [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4\(i\)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(i))

WE'VE OUTLINED THE REQUIREMENTS - HERE'S HOW WE CAN HELP

As CalCPA's Exclusive cybersecurity partner, we have created a Custom Cybersecurity Stack designed to keep your CPA firm up to snuff with these new FTC Safeguard regulations. Take the first step and book a 15-min consultation directly with our CEO, Scott Hagizadegan, so we can help fast-track the implementation of these measures.

[SCHEDULE HERE](#)