CTI TECHNOLOGY we make IT happen | MacHero

9 Elements of FTC Safeguards Security Program

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. **Each standard should be read in full before implementation.** Remember when reading the standards, your clients are the audience.

1 Designate a Qualified Individual

- In charge of overseeing/implementing information security program
- Can be 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)

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)

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)

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)

FTC SAFEGUARDS

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)

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)

7 Develop Continuous Improvement Cadence

- Evaluate information security program based on:
    - Testing
    - Materialchangesinyourorganization
    - Theresultsofariskassessment
- 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)

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)