FTC Safeguards Rule (Part 314)

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

Purpose

This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Scope

This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. Namely, this part applies to those "financial institutions" over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.

An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805.

More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.

They are referred to in this part as "You".

This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

FTC Safeguards Rule (Part 314) FTC.314.0 - Written Information Security Program

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.0 Written Information Security Program	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Guidance
Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC-PM-1 - Information Security Program Plan: Develop and disseminate an organization-wide information security program plan.

References
- 314.3 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314)
FTC.314.1 - Qualified Individual

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.1 Qualified Individual	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, Qualified Individual). The Qualified Individual may be employed by you, an affiliate, or a service provider.

To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

Guidance
The Qualified Individual can be an employee of your company or can work for an affiliate or service provider. The person doesn't need a particular degree or title. What matters is real-world know-how suited to your circumstances.

The Qualified Individual selected by a small business may have a background different from someone running a large corporation's complex system.

If your company brings in a service provider to implement and supervise your program, the buck still stops with you. It's your company's responsibility to designate a senior employee to supervise that person. If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program that protects your business.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC-PM-2 - Information Security Program Leadership Role: Appoint an information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.2 - Risk Based Information Security Program

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.2 Risk Based Information Security Program	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

Guidance
You can't formulate an effective information security program until you know what information you have and where it's stored.

After completing that inventory, conduct an assessment to determine foreseeable risks and threats internal and external to the security, confidentiality, and integrity of customer information. Among other things, your risk assessment must be written and must include criteria for evaluating those risks and threats.

Think through how customer information could be disclosed without authorization, misused, altered, or destroyed. The risks to information constantly morph and mutate, so the Safeguards Rule requires you to conduct periodic reassessments in light of changes to your operations or the emergence of new threats.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- FTC-PM-1 - Information Security Program Plan: Develop and disseminate an organization-wide information security program plan.
- FTC-PM-7 - Enterprise Architecture: Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.
- FTC-PM-9 - Risk Management Strategy: Develop a comprehensive strategy.
- FTC-PM-11 - Mission and Business Process Definition: Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
- FTC-RA-1 - Risk Assessment - Policy and Procedures: Develop, document, and disseminate to Appropriate Personnel.
- FTC-SA-2 - Allocation of Resources: Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314)
FTC.314.3 - Access Control Review

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.3 Access Control Review	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Periodically review access controls.

Guidance
Periodically review access controls to confirm that they permit access only to authorized users and limit authorized users access only to customer information that they need to perform their duties and functions.

Promotions, Transfers, and Terminations are often overlooked events that could enable access that is no longer needed for a specific job function. Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- FTC-AC-1 - Access Control - Policy and Procedures: Develop, document, and disseminate to Appropriate Personnel.
- FTC-AC-2 - Account Management: Define and document the types of accounts allowed and specifically prohibited for use within the system.
- FTC-AC-3 - Access Enforcement: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- FTC-AC-5 - Separation of Duties: a. Identify and document organization-defined duties of individuals requiring separation; and b. Define system access authorizations to support separation of duties.
- FTC-AC-6 - Least Privilege: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
- FTC-AC-24 - Access Control Decisions: Establish procedures to ensure access control decisions are applied to each access request prior to access enforcement.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.4 - Permit Access Only to Authorized Users

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.4 Permit Access Only to Authorized Users	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information.

Guidance
Are unique identifiers issued to individual users (usernames)?

Are the processes and service accounts that an authorized user initiates identified (scripts, automatic updates, configuration updates, vulnerability scans)?

Are unique device identifiers used for devices that access the system identified?

Make sure to assign individual, unique identifiers (usernames) to all users and processes that access company systems. Authorized devices also should have unique identifiers. Unique identifiers can be as simple as a short set of alphanumeric characters (LAP001 could refer to a laptop, LAP002 could refer to a different laptop). Prohibit the use of Shared accounts, all authorized users should have their own named accounts associated with them. Do not use Generic logins like Nurse or Receptionist.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- FTC-AC-1 - Access Control - Policy and Procedures: Develop, document, and disseminate to Appropriate Personnel.
- FTC-AC-2 - Account Management: Define and document the types of accounts allowed and specifically prohibited for use within the system.
- FTC-AC-3 - Access Enforcement: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- FTC-AC-5 - Separation of Duties: a. Identify and document organization-defined duties of individuals requiring separation; and b. Define system access authorizations to support separation of duties.

- FTC-AC-24 - Access Control Decisions: Establish procedures to ensure access control decisions are applied to each access request prior to access enforcement.

- FTC-IA-2 - Identification and Authentication (Organizational Users): Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.5 - Limit Authorized Users Access

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.5 Limit Authorized Users Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information.

Guidance
Do you only grant enough privileges to users to allow them to do their job?

Does the company restrict access to privileged functions and security information to authorized employees?

Does the Company have an access control policy?

The principle of least privilege applies to all users and processes on all systems, but it is critical to systems containing or accessing sensitive data. Least privilege restricts user access to only the machines and information needed to fulfill job responsibilities; and limits what system configuration settings users can change, only allowing individuals with a business need to change them.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- FTC-AC-1 - Access Control - Policy and Procedures: Develop, document, and disseminate to Appropriate Personnel.
- FTC-AC-2 - Account Management: Define and document the types of accounts allowed and specifically prohibited for use within the system.
- FTC-AC-3 - Access Enforcement: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- FTC-AC-5 - Separation of Duties: a. Identify and document organization-defined duties of individuals requiring separation; and b. Define system access authorizations to support separation of duties.

- FTC-AC-6 - Least Privilege: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

- FTC-AC-24 - Access Control Decisions: Establish procedures to ensure access control decisions are applied to each access request prior to access enforcement.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.6 - Identify and Manage Data, Personnel, Devices, Systems, and Facilities

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.6 Identify and Manage Data, Personnel, Devices, Systems, and Facilities	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.

Guidance
A fundamental step to effective security is understanding your company's information ecosystem.

Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted.

Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- FTC-CM-8 - System Component Inventory: Develop and document an inventory of system components that: 1. Accurately reflects the system.
- FTC-CP-2 - Contingency Plan: Develop a contingency plan for the system.
- FTC-CP-9 - System Backup: Conduct backups of user-level information contained in organization-defined system components at an organization-defined frequency consistent with recovery time and recovery point objectives.
- FTC-PS-7 - External Personnel Security: Establish personnel security requirements, including security roles and responsibilities for external providers.

- FTC-RA-9 - Criticality Analysis: Identify critical system components and functions by performing a criticality analysis for organization systems, system components, or system services when an architecture or design is being developed, modified, or upgraded.

- FTC-SA-9 - External System Services: Require that providers of external system services comply with organizational security and privacy requirements.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.7 - Encrypt all Customer Information Held or Transmitted

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.7 Encrypt all Customer Information Held or Transmitted	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Protect by encryption all customer information held or transmitted by you, both in transit over external networks and at rest.

To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual.

Guidance
Information at rest means information that is not moving through the network; typically this means data currently stored on hard drives, media, and mobile devices.

Transmission of customer information should use secure protocols (encryption).

All remote access of customer information should be by secure methods only. Unprotected customer information should not be sent via unencrypted emails, only in encrypted password protected attachments to known entities if no other secure method is available. If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC-MP-1 - Media Protection - Policy and Procedures: Develop, document, and disseminate to Appropriate Personnel.
- FTC-MP-3 - Media Marking: Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
- FTC-MP-4 - Media Storage: Physically control and securely store digital and/or non-digital media within organization-defined controlled areas.

- FTC-MP-5 - Media Transport: Protect and control system media during transport outside of controlled areas using encryption.
- FTC-MP-6 - Media Sanitization: Sanitize system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures.
- FTC-MP-7 - Media Use: a. Restrict the use of portable storage devices on organization-defined systems; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.
- FTC-SC-1 - System and Communications Protection - Policy and Procedures: Develop, document, and disseminate to Appropriate Personne.
- FTC-SC-8 - Transmission Confidentiality and Integrity: Protect the confidentiality and integrity of transmitted information.
- FTC-SC-28 - Protection of Information at Rest: Protect the confidentiality and integrity of the following information at rest: PII.

References

- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.8 - Adopt Secure Development Practices

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.8 Adopt Secure Development Practices	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.

Guidance
If using in-house developed applications: Leverage the Secure Software Development Framework (SSDF) developed by NIST.

The Secure Software Development Framework (SSDF) is a set of fundamental, sound, and secure software development practices based on established secure software development practice documents from organizations such as BSA, OWASP, and SAFECode.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC.SFR-314.8C - Adopt Secure Development Practices: Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.

References
- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314)
FTC.314.9 - Multi-factor Authentication

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.9 Multi-factor Authentication	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.

Guidance
Implement a combination of two or more factors of authentication to verify an individual's identity regardless of how the user is accessing the account. The implementation of multi-factor authentication will depend on the environment and business needs.

Although two-factor authentication directly on the computer is most common, there are situations (multi-factor identification for a system that cannot be altered) where additional technical or physical solutions can provide security.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC.SFR-314.9C - Multi-factor Authentication: Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.
- FTC-IA-1 - Identification and Authentication - Policy and Procedures: Develop, document, and disseminate to appropriate personnel.
- FTC-IA-2 - Identification and Authentication (Organizational Users): Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
- FTC-IA-3 - Device Identification and Authentication: Uniquely identify and authenticate organization-defined devices before establishing a network connection.

References
- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.10 - Secure Disposal of Customer Information

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.10 Secure Disposal of Customer Information	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Develop, implement, and maintain procedures for the secure disposal of customer information.

Guidance
Customer information in any format must be securely disposed of no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Any format refers to a broad range of items that store information, including paper documents, disks, tapes, digital photography, USB drives, CDs, DVDs, and mobile phones. It is important to know what information is on media so that you can handle it properly.

If there is sensitive data, you or someone in your company should either: shred or destroy the device before disposal so it cannot be read, or clean or purge the information, if you want to reuse the device.

The deletion function in most operating systems allows deleted data to be recovered, so instead, a dedicated secure deletion function or application should be used to make data unrecoverable.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC-MP-6 - Media Sanitization: a. Sanitize system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

References
- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC Safeguards Rule (Part 314) FTC.314.11 - Review Data Retention Policy

FTC Safeguards Rule (Part 314)	Other Requirements
FTC.314.11 Review Data Retention Policy	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Periodically review your data retention policy to minimize the unnecessary retention of data.

Guidance
Review your data retention policies at least annually.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- FTC.SFR-314.11C - Review Data Retention Policy: Periodically review your data retention policy to minimize the unnecessary retention of data.

References
- 314.4 Standards for safeguarding customer information - https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

Truncated Sample Report