

WAC 208-630-715 What are the minimum requirements of an information security program required by the Federal Safeguards Rule implementing the Gramm-Leach-Bliley Act? (1) Generally, applicants and licensees must have a written program appropriate to the company's size and complexity, the activity conducted, and the sensitivity of information at issue. The program must ensure the information's security and confidentiality, protect against anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of the information.

(2) Specifically, at a minimum the plan described in subsection (1) of this section must:

(a) Designate an employee or employees to coordinate the information security program;

(b) Identify and assess the risks to customer information;

(c) Design and implement safeguards to control the risks identified in the risk assessment and regularly monitor and test the safeguards;

(d) Select service providers that can maintain appropriate safeguards and oversee their handling of customer information; and

(e) At least annually evaluate and adjust the program in light of relevant circumstances, including changes in business operations, or the results of testing and monitoring the effectiveness of the implemented safeguards.

(3) The information security plan must be maintained as part of your books and records.

(4) Compliance with the federal Gramm-Leach-Bliley Act and Regulation P, 12 C.F.R. Part 1016, will be deemed compliance with this subsection.

(5) For more information access the FTC website on the Safeguards Rule at: <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> and see 16 C.F.R. 314.

[Statutory Authority: Chapter 43.320 RCW, RCW 31.45.200. WSR 16-10-046, § 208-630-715, filed 4/29/16, effective 6/1/16.]