ALABAMA DEPARTMENT OF INSURANCE
ADMINISTRATIVE CODE

CHAPTER 482-1-126
STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

TABLE OF CONTENTS

482-1-126-.01 Preamble.

(1) This chapter establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

(2) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of records or information

that could result in substantial harm or inconvenience to a customer.

(3) Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by regulation with respect to persons engaged in providing insurance.

(4) Section 507 provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This chapter requires that the safeguards established pursuant to this chapter shall apply to nonpublic personal financial information.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.02 Authority. This chapter is adopted pursuant to Sections 27-2-17 and 27-7-44, Code of Ala. 1975, and Title V of the Gramm-Leach-Bliley Act (15 U.S.C. §§6801-6827) (hereinafter "GLBA").

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.03 Definitions. For purposes of this chapter, the following definitions apply:

(a) CUSTOMER. A customer of the licensee as the term customer is defined in Rule 482-1-122-.04.

(b) CUSTOMER INFORMATION. Nonpublic personal information as defined in Paragraph S. of Rule 482-1-122-.04 about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

(c) CUSTOMER INFORMATION SYSTEMS. The electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

(d) LICENSEE. A licensee as that term is defined in Paragraph Q. of Rule 482-1-122-.04, except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to surplus line business conducted pursuant to Chapter 10 of Title 27, Code of Ala. 1975. This chapter does not apply persons operating pursuant to Chapter 32 of Title 8 (Service Contracts).

(e) SERVICE PROVIDER. A person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.04 Information Security Program. Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.05 Objectives Of Information Security Program. A licensee's information security program shall be designed to do all of the following:

(a) Ensure the security and confidentiality of customer information.

(b) Protect against any anticipated threats or hazards to the security or integrity of the information.

(c) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.
Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.06 Examples Of Methods Of Development And Implementation. The actions and procedures described in Rules 482-1-126-.07 through 482-1-126-.10, inclusive, are examples of methods of implementation of the requirements of Rules 482-1-126-.04 and 482-1-126-.05. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Rules 482-1-126-.04 and 482-1-126-.05.
Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.07 Assess Risk. The licensee:

(a) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.

(b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

(c) Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.08 Manage And Control Risk. The licensee:

(a) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities.

(b) Trains staff, as appropriate, to implement the licensee's information security program.

(c) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: **New Rule:** May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.09 Oversee Service Provider Arrangements. The licensee:

(a) Exercises appropriate due diligence in selecting its service providers.

(b) Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.10 Adjust The Program. The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.
Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.11 Determined Violation. A licensee violating this chapter may be subject to the suspension or revocation of his, her or its license or certificate of authority in accordance with Subsection (e) of Section 27-2-17, Code of Ala.1975.
Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.

482-1-126-.12 Effective Date. This chapter shall become effective upon its approval by the Commissioner of Insurance and upon its **having been on file as a public document in the office of** the Secretary of State for ten days. Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this chapter by December 1, 2003.

Author: Commissioner of Insurance
Statutory Authority: Code of Ala. 1975, §§27-2-17, 27-7-44; 15 U.S.C. §§6801-6827.
History: New Rule: May 6, 2003; effective May 16, 2003. Filed with LRS May 7, 2003. Rule is not subject to the Alabama Administrative Procedure Act.