Cyber Security Plan

Overview

Financial institutions must have stringent security to protect themselves and their customers. A lot of the security is mandated by federal agencies to help protect citizens. Most of this document will explain laws and regulations imposed by these agencies and how to put the in use. These rules and regulations can be found on the FDIC website at https://www.fdic.gov/resources/bankers/information-technology/

Federal Deposit Insurance Act (FDI Act)

The FDI Act requires banking agencies to establish operational and managerial standards, compensation standards, and standards relating to asset quality, earnings, and stock valuation. While a lot of this has to to with how the business is ran there are many system requirements listed.

- Effective risk assessment
- Timely and accurate financial, operational and regulatory reports
- Adequate procedures to safeguard and manage assets
- Adequate monitoring of the system of internal controls through an internal audit function
- Adequate testing and review of information systems
- Adequate documentation of tests and findings and any corrective actions
- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer
- Ensure the proper disposal of customer information and consumer information
- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems
- Design 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 institution's activities
- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access
- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program

- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
- Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures
- Regularly test the key controls, systems and procedures of the information security program
- Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information
- Each institution shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology