

Customer Information Security

Protecting customers' personal data is only one facet of the Gramm-Leach-Bliley Act. In accordance with the Act, the Safeguards Rule mandates that financial institutions must document, implement and uphold an information security plan that properly protects customers' personal data. Part of this requirement entails having an employee training program in place that addresses information security issues.

The BankersEdge Customer Information Security curriculum is a set of core courses that covers key policies and procedures all banks must adopt to help ensure compliance with the Act. Taken in a series, the 22 topics that comprise this curriculum provide a sound foundation with which to support GLBA compliance in your organization.

A Clean Desk Policy	156-1V4R7
Explore instituting a policy that addresses employees' housekeeping habits at work, from how to handle unattended documents and storage media to the document disposal in the waste bin. Shared hardware usage issues are also discussed in this module.	
Customer Requests	156-3V4R7.2
Establish procedures for responding to lawfully authorized requests for release of confidential data.	
Data Encryption Standards	156-4V4R7.2
Learn about standards for encoding/decoding customer data.	
Incident Response Program	156-5V4R7.2
Explore the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information — a program developed to respond to unauthorized access to customer information, including required notifications.	
Information Disposal	156-6V4R7.2
Review the legal requirements that affect different types of documents that contain sensitive information, and the time limits set for shredding and disposal of sensitive information.	
Interactive Voice Response Systems	156-8V4R7.2
How does the interactive voice response system work? Find out how IDs and PINs ensure system security.	
Internet Banking Security	156-7V4R7.2
Establish best-practice protocols including forced password changes, lockouts and multi-factor (strong) authentication.	
Intrusion Detection and Firewall Security	156-9V4R7.2
Gain a better understanding of access attempts from outside hackers, and the systems used to detect and deter such activities.	

Laptop and PDA Security	156-10V4R7.2
Brush up on laptop- and cell phone-related security issues.	
Magnetic File Backup and Storage	156-11V4R7.2
Hard drives, tapes and cartridges are the primary means banks employ for storing confidential operational and customer data. This module examines the issues around the use of common storage media.	
Media and Equipment	156-12V4R7.2
How does your bank remove confidential data from media? Learn about controls you must put in place to ensure all media is properly tracked and destruction is logged.	
Network Component Security	156-13V4R7.2
Take a closer look at the types of security issues connected with a bank's network hardware.	
Passwords	156-14V4R7.2
Discover best practices for selecting passwords and controlling access to workstations.	
PC Software Controls	156-15V4R7.2
Learn how to establish policies for employees' computers that set expectations in relation to unauthorized modifications by authorized users leading to incompatibility issues, viruses, and non-professional usage.	
PINs	156-16V4R7.2
Explore issues related to customers' personal identification numbers (PINs), and the banking products and services they permit access to.	
Remote Access Standards	156-17V4R7.2
Gain a better understanding of how to enforce remote access standards when working with a service provider.	
Securing Customer Information	156-18V4R7.2
Consider compliance with the GLBA from a bank IT perspective.	
Securing Non-Public Areas	156-19V4R7.2
Learn about operational issues in non-public areas, including contractor/service personnel, badges and visitor logs.	
Security System Issues	156-20V4R7.2
Review FAX, e-mail and Internet systems, as well as acceptable use, confidentiality and professional use policies.	
Virtual Private Network Security	156-21V4R7.2
Learn more about information security guidelines for VPN use.	
Virus and Spyware Prevention	156-22V4R7.2
Learn how to prevent individual PC and file server destruction, as well as unplanned network downtime due to attacks from malicious programs.	