Gramm-Leach-Bliley Policy Procedures

Guidance for Implementing American University's Information Security Plan

I. How to Comply

The requirements of the Gramm-Leach-Bliley Act and its implementing regulations and American University's Information Security Plan are intended to be flexible. This guidance is not intended to be comprehensive and each Covered Office must assess all areas of operation and implement appropriate safeguards.

II. Securing Information

In general, each Covered Office should take reasonable and logical measures necessary to maintain the security of Covered Information. In developing safeguards, a Covered Office should consider all areas of its operation, including three areas that are particularly important to information security; **employee management and training; paper and electronic information systems**; and **managing system failures**. The following practices in these areas should be considered.

Employee Training and Management

The success or failure of the university's Information Security Plan depends largely on the employees who implement it. You may want to:

a. Check references prior to hiring employees who will have access to Covered Information.
b. Have each employee sign a confidentiality agreement which includes a promise to comply with the university's confidentiality and security standards for handling Covered Information.
c. Train employees to take basic steps to maintain the security, confidentiality and integrity of Covered Information, such as;

- locking rooms and file cabinets where paper records are kept
- using password-activated screensavers
- using unique passwords (non-dictionary words and/or number combinations)

- changing passwords periodically and not posting passwords near employees' computers
- encrypting Covered Information when it is transmitted electronically over networks or stored on-line
- referring calls or other requests for Covered Information to designated individuals who have had safeguards training
- recognizing any fraudulent attempt to obtain Covered Information and reporting it to appropriate internal university offices and law enforcement agencies.

d. Instruct and regularly remind all employees of the university policy, the legal requirement, and your offices' practices and procedures to keep Covered Information secure and confidential. You may want to provide employees with a detailed description of the kind of covered Information you handle and post reminders about their responsibility for security in areas where such information is stored—in file rooms, for example.
e. Limit access to Covered Information to employees who have a business reason for seeing it. For example, grant access to Covered Information files to employees who respond to customer inquiries, but only to the extent they need to do their jobs.
f. Impose disciplinary measures for any breaches; and
g. Terminate employee's computer, email, and other information system access immediately upon termination of employment.

Paper and Electronic Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal of electronic and, where applicable, paper records. Here are some suggestions on how to maintain security throughout the life cycle of Covered Information.

a. Store records in a secure area. Make sure only authorized employees have access to the area.

- store paper records in a room, cabinet, or other container that is locked when unattended
- maintain a "clean desk" policy
- ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or flood

- store electronic Covered Information on a secure server that is accessible only with a password—or has other security protections—and is kept in a physically-secure area
- don't store Covered Information on a machine with an Internet connection
- maintain secure back-up media and keep archived data secure, for example, by storing off-line or in a physically-secure area.

b. Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit Covered Information. Specifically,

- if you collect credit card information or other sensitive financial data, use a secure connection so that the information is encrypted in transit
- if you access Covered Information from a remote location, use a secure connection so that the information is encrypted in transit
- if you collect Covered Information directly from customers, make secure transmission automatic and caution customers against transmitting sensitive data, like account numbers, via electronic mail
- if you must transmit covered Information by electronic mail, ensure that such messages are password protected so that only authorized employees have access.

c. Dispose of Covered Information in a secure manner.

- designate an employee responsible for records retention to supervise the disposal of records containing Covered Information
- shred Covered Information recorded on paper
- promptly dispose of outdated Covered Information
- refer to the university's records retention and disposal policy for further guidance in this area.

d. Use appropriate oversight or audit procedures to detect the improper disclosure or theft of Covered Information.

e. Maintain a close inventory of your computers.

Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions:

a. Maintain up-to-date and appropriate programs and controls by:
   - following a written contingency plan to address any breaches of your physical, administrative or technical safeguards
   - checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities
   - using anti-virus software that updates automatically
   - maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations
   - providing central management of security tools for your employees and passing along updates about any security risks or breaches.

b. Take steps to preserve the security, confidentiality and integrity of Covered Information in the event of a computer or other technological failure. For example, back up all customer data regularly.

c. Maintain systems and procedures to ensure that access to Covered Information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the university electronically.

d. Promptly notify the Information Security Plan Coordinator (Executive Director of Risk Management and Safety Services, or the Chief Information Officer in the event of a security breach involving electronic records) if Covered Information has been subject to loss, damage or unauthorized access. Consider appropriate mitigation steps.

Questions

Any questions related to these guidelines should be directed to the Information Security Plan Coordinator at pat@american.edu or by phone at x3284.