AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Data Breach Notification Policy

Policy Category: Operational Policies: Ethics, Integrity and Legal Compliance Policies: Information Technology Policies

Subject: To comply with the Gramm-Leach-Bliley Act, DC Consumer Personal Information Security Breach Notification Act, Payment Card Industry Data Security Standard, and other applicable local and federal data protection and notification regulations.

Office Responsible for Review of this Policy: Office of Finance and Treasurer

Procedures: Contact Executive Director of Risk Management (x3284 or e-mail dnichols@american.edu) or CIO (x2612 or e-mail dswartz@american.edu)

Related University Policies: Computer Use and Copyright Policy; Cardholder Data Security Policy; Gramm-Leach-Bliley Policy; Information Technology Security Policies; Identity Theft Prevention Policy; Records Retention and Disposal Policy

---

I. SCOPE

This policy applies to all offices that collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifying information (PII) of students, faculty, and staff.

II. POLICY STATEMENT

American University maintains an information security plan to protect the security, confidentiality, and integrity of Personal Information of students, staff, and faculty. As part of its information security plan, the University will notify affected individuals of a data security breach as required by the relevant local, state, or federal laws.

III. DEFINITIONS

"Covered Information" or "Personal Information" are used interchangeably—sensitive, non-public, personally identifiable information of an individual. These include, but are not limited to

a. an individual's name (first name or first initial and last name), or phone number, or address, in conjunction with any of the following data elements:
    - social security number
    - credit and debit card information
    - income and credit history
    - bank account information
    - driver's license number
    - tax return
    - asset statement
b. any number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.

Covered Information includes both paper and electronic records.

IV. POLICY

Implementing Safeguards

The following safeguards must be implemented by offices which maintain or handle Covered Information:

- Require all employees to immediately notify their supervisor of any actual or suspected security breach involving files containing Personal Information. For example, a breach may involve a lost or stolen computer or other device containing unencrypted Covered Information or the access of Personal Information by unauthorized individuals. If employees are uncertain whether there has been a breach, they must be advised to report the event to their supervisor.
- Regularly train employees, including all temporary, contract, or work-study employees, to take basic steps to maintain the security, confidentiality and integrity of personal 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) in accordance with the University IT Security Policy
    - changing passwords periodically and not posting passwords on employees' computers in accordance with the University IT Security Policy
    - never sharing passwords with others
    - encrypting personal information when it is transmitted electronically over networks or stored on-line
    - encrypting PII when the data is stored on AU owned systems, in accordance with the University IT Security Policy.

- referring calls or other requests for personal information to designated individuals within the department, university registrar, or human resources
- requiring all third-party vendors/contractors having access to Covered Information to exercise reasonable care in the handling of Personal Information and to implement commercially reasonable policies, procedures and systems to protect the confidentiality, security, and integrity of personal information and to detect the occurrence of a data breach. This requirement must be imposed on the third-party by a written provision in a contract.

Note: Contact the Office of Information Technology HelpDesk at 202-885-2550 and ask for an information security consultation on handling sensitive electronic data.

Reporting of Data Breach

If a data breach has occurred or is suspected, supervisors must immediately report the event to the Executive Director of Risk Management (x3284 or e-mail dnichols@american.edu or the Chief Information Officer (x2612or e-mail dswartz@american.edu).

Evaluation regarding whether there has been a data breach of Personal Information requiring notification to affected individuals will be determined by the Risk Management Office, in consultation with the Office of Information Technology and other relevant offices. The Risk Management Office will assist offices or departments in which the breach occurred in drafting any needed notification.

V. EFFECTIVE DATE: March 30, 2009
Last reviewed March, 2011.
Revised August 2016.

This document was approved and signed by

Doug Kudravetz
Vice President and Treasurer

David Swartz
Vice President and Chief Information Officer