AMERICAN UNIVERSITY
WASHINGTON, DC

University Policy: Data Classification Policy

Policy Category: Operational Policies

Subject: Classification of University Data for Security and Confidentiality

Responsible Executive: Chief Financial Officer, Vice President & Treasurer

Office Responsible for Annual Review of this Policy: Office of Finance and Treasurer and Office of Information Technology

Related University Policies: Information Technology Security Policy, Responsible Use of University Technology Resources, Health Insurance Portability and Accountability Privacy Act, Confidentiality of Student Records Policy, Records Retention and Disposal Policy

I. SCOPE

This policy governs the privacy, security, and integrity of university data, especially confidential data, and the responsibilities of institutional units and individuals for such data regardless of where that data resides (e.g., AU owned systems, personal devices, or AU approved external hosting services). The policies and procedures provided herein apply to all University faculty, staff, students, visitors, and contractors.

II. POLICY STATEMENT

American University maintains data essential to the performance of university business. All members of the university community have a responsibility to protect university data from unauthorized generation, access, modification, disclosure, transmission, or destruction.

The objective of this policy is to assist AU employees in the assessment of data to determine the level of security, which must be implemented to protect that data whether it is in paper copy or on the information system for which they are responsible during the course of university business. All university data are classified into three levels of sensitivity, Confidential, Official Use Only, and Unrestricted. Once data has been classified, appropriate safeguards must be implemented to protect data from theft, loss, and/or unauthorized disclosure, use, access, and/or destruction.

Providing the community with an opportunity to share and use data with care is one of the great benefits of our university. However, misuse, misinterpretation, or unnecessary restrictions on access to that data can diminish this benefit. Although a large portion of university data is available for the public, some data have restrictions due to privacy protections mandated by federal and local regulations and laws, contractual agreements, ethical considerations, and proprietary worth. To comply with these mandates and protect the university community, the university has the right and obligation to protect: the

confidentiality, integrity, and availability of data under its purview. Data can also be classified based on the application of "prudent stewardship", where there is no reason to protect the data other than to reduce the possibility of harm or embarrassment to individuals or to the institution. The classification level assigned to data will provide guidance to data custodians and others who may collect, process, or store data.

III. DEFINITIONS

Confidential Data: Confidential data are considered the most sensitive and require the highest level of protection. Confidential data includes data that the university must keep private under federal, local, and state laws, contractual arrangements, or based on its proprietary worth. Confidential data may be disclosed to individuals on a strict need-to-know basis or as permitted under relevant law or contractual arrangement.

Official Use Only Data: Official Use Only data is generally private to the University. Access is limited to AU community members on a need-to-know basis and it is not generally available to parties external to American University.

Unrestricted Data: Unrestricted Data has no legal or other restrictions on access or usage and may be open to the university community and the general public.

IV. POLICY

A. DATA MANAGEMENT

1. General.

All members of the university community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the university, irrespective of the medium on which the data reside, the location of that data, and its format (such as in electronic, paper, or other physical form).

2. Data Classification.

Departments must classify data into the appropriate category. University data are assets belonging to the institution and should be classified according to the risks associated with the data being stored or processed. Confidential Data are considered the most sensitive and require the highest level of protection to prevent unauthorized disclosure or use. Data, which are not confidential, may be given proportionately less protection. This approach allows American University to apply more appropriate levels of resources to the protection of the assets based upon need.

Data are generally stored in collections (i.e., databases, files, tables, etc.) Often these collections do not segregate the more sensitive data elements of a collection from the less sensitive data. Therefore, in determining the classification category, the most sensitive data element in the collection is used to classify the entire collection.

Examples of Confidential Data include:

- Credit card numbers
- Medical Records
- Disability Records
- Passwords
- Student Records
- Social Security Numbers
- Personnel and/or Payroll Records
- Specific Donor Information

Examples of Official Use Only Data include:

- Employment Data
- University Partner or Sponsor Information
- Research Records
- Library Transactions
- Financial Transactions
- Pre-approved official meeting minutes
- Drafts of official documents

The examples in this category assume that no more restrictive confidentiality agreement, legal requirement, or proprietary worth exists.

Examples of Unrestricted Data include:

- American University's website
- Publicly Posted Press Releases
- Publicly Posted Schedules of Classes or Course Catalog
- Publicly Posted Interactive University Maps, Newsletters,
- Newspapers, Job announcements, and Magazines

B. DATA SAFEGUARDS.

Departments must implement appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of university data. Confidential Data are considered the most sensitive and require the highest level of protection. This policy provides examples of safeguards. However, departments may implement procedures more restrictive than the ones identified in this policy.

1. General Safeguards for All Data

a. Using the categories Confidential, Official Use Only, or Unrestricted, all University data must be classified, as soon as possible after the creation or acceptance of ownership by the University.

b. Following initial classification, University data must remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law or other relevant circumstances.

c. Classifications assigned to University data must be reviewed at least once every three (3) years and reclassified based on changing usage, sensitivities, law, or other relevant circumstances. (E.g. data currently classified as Official Use Only Data may only be elevated to Confidential with the passing of local state or federal laws).

d. Data must be protected in accordance with the security controls specified for the classification level that it is assigned.

e. The classification level and associated protection of replicated data must remain consistent with the original data [e.g. (i) confidential HR data copied to a CD-ROM, or other removable-media (e.g. flash drive), or from one server to another, retains its confidential classification; (ii) printed copies of Confidential Data is also confidential].

f. Any physical or logical collection of data, stored, or during electronic transfer (e.g. file, database, in "the Cloud", emails and attachments, filing cabinet, backup media, electronic memory devices, sensitive operation logs or configuration files) containing differing classification levels must be classified as a whole at the highest data classification level within the collection. Any data subset that has been separated from any such collection must be protected in accordance with the protection specified for the classification level of the data subset if assigned; otherwise the data subset retains the classification level of the original collection and requires the same degree of protection.

g. Destruction of data (electronic or physical) or systems storing data must be done in accordance with the University's Records Retention and Disposal Policy.

h. Before systems or media are reused they should be erased according to University guidelines to ensure no residual data.

2. Safeguards for Confidential Data

a. Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.

b. Must be clearly labeled Confidential Data.

c. When stored in an electronic format must be protected with strong passwords and stored on servers that have protection and encryption measures.

d. May only be disclosed on a strict need-to-know basis or as permitted by

law or contractual arrangement and consistent with applicable university policies.

e. Must be stored only in a locked drawer or room or an area where access is controlled using sufficient physical access control measures to detect and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

f. When sent via fax, must be sent only to a previously established and used fax number or one that has been verified as using a secured location.

g. Must not be posted on any website unless secured authentication methods are used and are assessed by the Office of the Chief Information Security Officer.

h. Must be destroyed when no longer needed in accordance with University policies.

3. Safeguards for Official Use Only Data

a. Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.

b. May only be disclosed to members of the university community who have a legitimate purpose for accessing such data.

c. Must be stored in a controlled environment (i.e. file cabinet or office where physical controls are in place to prevent disclosure) when not in use.

d. Must not be posted on any public website unless secured authentication methods are used.

e. Must be destroyed when no longer needed in accordance with the University Records Retention and Disposal Policy.

4. Safeguards for Unrestricted Data Unrestricted data, while subject to university disclosure rules, are available to all members of the university community and to all individuals and entities external to the university community. While the requirements for protection of Unrestricted Data are less restrictive than for Official Use Only Data, protection considerations should be applied to maintain data integrity and prevent unauthorized modification of such data. Safeguards for Unrestricted Data may include:

a. Should reside on an appropriately secured host.

b. Should have appropriate integrity protection.

c. Should have redundant systems to maintain availability as appropriate.

d. Should be retained according to public record requirements.

e. Should have an appropriate recovery plan.

V. COMPLIANCE

Violations of this policy may result in disciplinary action up to and including termination of employment.

VI. EFFECTIVE DATE AND REVISIONS:

This policy was effective April 7, 2009.

Reviewed March 2011; August 2014.
Revised July 2016.