	Responsible University Official: Chief Information Officer **Responsible Office:** Information Systems and Services **Origination Date:** April 12, 2004 **Last Amended Date:** December 6, 2005

DATA CLASSIFICATION SECURITY POLICY

Policy Statement

All members of the university community have a responsibility to protect university data from unauthorized generation, access, modification, disclosure, transmission or destruction, and are expected to be familiar with and comply with this policy. Violations of this policy can lead to disciplinary action up to and including dismissal, expulsion, and/or legal action. Any known violations of this policy are to be reported to the Office of the Assistant Vice President for Information Security and Compliance Services.

Reason for Policy/Purpose

To educate the university community about the importance of protecting data generated, accessed, transmitted and stored by the university, to identify procedures that should be in place to protect the confidentiality, integrity and availability of university data, and to comply with local and federal regulations regarding privacy and confidentiality of information.

Who Needs To Know This Policy

Faculty, staff and students

Table of Contents

Policy/Procedures

I. RESPONSIBILITY FOR DATA MANAGEMENT

Data is a critical asset of the university. 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 resides and regardless of format (such as in electronic, paper or other physical form).

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of university data in compliance with this policy.

Data owned, used, created or maintained by the university is classified into the following three categories:

- Public
- Official Use Only
- Confidential

Departments should carefully evaluate the appropriate data classification category for their information.

When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements. Nothing in this policy is intended to identify a restriction on the right of departments to require policies and/or procedures in addition to the ones identified in this document.

II. DATA CLASSIFICATIONS

A. PUBLIC DATA

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to university disclosure rules, is available to all members of the university community and to all individuals and entities external to the university community.

By way of illustration only, some examples of Public Data include:

- Publicly posted press releases
- Publicly posted schedules of classes

- Publicly posted interactive university maps, newsletters, newspapers and magazines

B. OFFICIAL USE ONLY DATA

Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the university community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of Official Use Data include:

- Employment data
- University partner or sponsor information where no more restrictive confidentiality agreement exists
- Internal telephone books and directories

Official Use Only data:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.

- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.

- Must not be posted on any public website.

- Must be destroyed when no longer needed subject to the university's Records Management Policy. Destruction may be accomplished by:
  - o "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.

  - o Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the university's Electronic Equipment Recycling Policy.

C. CONFIDENTIAL DATA

Confidential Data is information protected by statutes, regulations, university policies or contractual language. Managers may also designate data as confidential.

Confidential Data may be disclosed to individuals on a need-to-know basis only.

Disclosure to parties outside the university should be authorized by executive management and/or the Office of the Senior Vice President and General Counsel.

By way of illustration only, some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data
- Social Security Numbers
- Personnel and/or payroll or records
- Bank account numbers and other personal financial information
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Confidential data:

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided by Division of Information Technology in order to protect against loss, theft, unauthorized access and unauthorized disclosure.

- Must not be disclosed to parties without explicit management authorization.

- Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

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

- Must not be posted on any public website.

- Must be destroyed when no longer needed subject to the university's Records Management Policy. Destruction may be accomplished by:
  - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
  - Electronic storage media shall be sanitized appropriately by degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the university's Electronic Equipment Recycling Policy.

The Office of the Assistant Vice President for Information Security and Compliance Services must be notified in a timely manner if data classified as confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the university's information systems has taken place or is suspected of taking place.

III.   DATA CLASSIFICATION ROLES AND RESPONSIBILITIES

The Division of Information Technology is the primary entity charged with developing policy and procedures subordinate to and in support of this policy.

The Office of the Chief Information Officer is charged with the promotion of security awareness within the university community, as well as responsibility for the creation, maintenance, enforcement and design of training on relevant security standards in support of this policy. The Chief Information Officer will receive and maintain reports of incidents, threats and malfunction that may have a security impact on the university's information systems, and will receive and maintain records of actions taken or policies and procedures developed in response to such reports. The Chief Information Officer will assist Internal Audit, as appropriate, in conducting periodic audits to determine university compliance with this policy.

The University Compliance & Privacy Office will facilitate distribution of this policy, will assist in the investigation of policy breaches, and will administer the university's 24 hour Regulatory Compliance Help and Referral Line (1-888-508-5275), which provides a confidential method for reporting instances of suspected misconduct or violations of law or university policies.

The Office of the Senior Vice President and General Counsel will review procedures issued under authority of this policy for compliance with applicable regulations. The Office of the Senior Vice President and General Counsel will also respond to court ordered releases of information.

Website Address for This Policy

GW University Policies

Contacts

Subject	Contact	Phone	E-mail
Security Questions	Division of IT Help Desk http://it.gwu.edu	202-994-4948	ithelp@gwu.edu
	http://helpdesk.gwu.edu		
Reporting Security Incidents	Information Security Services	703-726-4412	abuse@gwu.edu
	http://it.gwu.edu/tnav/stayconnected/security/ReportSecurityIncident/		
	Compliance & Privacy Office	202-994-3386	comply@gwu.edu

Regulatory Compliance
Help and Referral Line   1-888-508-5275

Related Information

Family Educational Rights and Privacy Act of 1974 (FERPA)
Health Insurance Information Portability and Accountability Act (HIPAA)
George Washington University Privacy Policy Statement
Information Security Policy
Privacy of Student Records Policy
Records Management Policy
Social Security Number Usage Policy

Who Approved This Policy

Robert A. Chernak, Senior Vice President for Student and Academic Support Services
Louis H. Katz, Executive Vice President and Treasurer
Donald R. Lehman, Executive Vice President for Academic Affairs
Beth Nolan, Senior Vice President and General Counsel
John F. Williams, Provost and Vice President for Health Affairs

Who Approved This Policy

Origination Date: April 12, 2004

Last Amended Date: December 6, 2005

Next Review Date: June 30, 2013