

Date: February 13th, 2008

To: Staff and Faculty
College of Social & Behavioral Sciences

From: Georgios Mousouros
Information Security Liaison
College of Social & Behavioral Sciences

Re: Data Classification

Purpose

The purpose of this document is to outline the Data Classification at the College of Social and Behavioral Sciences.

Scope

This policy applies to all users including faculty, staff, students and guest users of the College of Social and Behavioral Science computer networks, equipment, or connectivity resources.

Availability

This document is freely available to everyone. Copies may be obtained from the web at: <http://www.sbs.arizona.edu/links/sbstech/security>

Revision History

First Draft: February 13th, 2008

I. Purpose

The purpose of this Data Classification document is to provide a framework for protecting the college of Social and Behavioral Sciences information resources. Information resources are assets of the University and must be classified by the sensitivity, confidentiality, availability and integrity.

II. Definitions

Data: Numerical or other information represented either in a physical form or a form suitable for electronic processing or storage.

Public Data: Information that is open to the general public.

Sensitive Data: Information whose access must be guarded due to proprietary, ethical or privacy considerations i.e.

Employee and Student IDs

Actions pertaining to renewal/termination of employment

Library Patron Records

Confidential Data: Information protected because of protective statutes, policies or regulations i.e.

SSNs and Student IDs

Driver Licenses

Student Financial Information

Birth dates

Account Numbers

P-cards

Insurance Information

Grades

Counseling/Mental Health Records

Medical Records

Disability Records

Non-disclosure Agreements

Institutional data: All data created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf.

FERPA: Family Educational Rights and Privacy Act of 1974, also known as the Buckley Amendment. The federal law that protects the privacy of student academic records.

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

GLBA: Gramm-Leach Bliley Act. The federal law that protects consumer's personal and financial information held by financial institutions, including universities.

<http://www.ftc.gov/bcp/online/pubs/buspubs/glbshort.shtm>

HIPAA: Health Insurance Portability and Accountability Act of 1996. Protects the security of individually identifiable health information.

<http://aspe.hhs.gov/admsimp/pl104191.htm>

III. Data Management

Data User

The Data User is a person, organization or entity that interacts with data for the purpose of performing an authorized task. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with policy.

Data Owner

The Data Owner is normally the person responsible for, or dependent upon the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

Data Custodian

The Data Custodian maintains the protection of data.