Standard Operating Procedure: Data Classification

Approved: 02-25-2013
Revised: 04-27-2018

Purpose

Define and standardize the steps necessary to classify data into defined categories and assign protection based on identified risk. This enables Data Owners, working in conjunction with IT Services, to ensure that data is managed and stored in and secure and efficient.

Definitions

Data Classification: The act of assigning a level of sensitivity or confidentiality, as well as an owner to each data object.
Object: A resource accessed by a subject, such as a computer system, file, folder, memory, etc. Objects are passive.
Personally Identifiable Information (PII): Information that can be used on its own or with other data to identify, contact, or locate a single person, or to identify a single person in context, or to de-anonymize anonymous data.
Subject: Accesses an object, such as a person, process, system, or system account. Subjects are active.
University Data: Information that is in the possession or control of an individual (owner, custodian, user) by virtue of that person's employment or affiliation with the University.
Data Owner: A person responsible for a business function and for determining controls and access to information resources supporting that business function. Typically, not IT Services.
Data Custodian: Person responsible for implementing owner-defined controls and access to an information resource. This may include employees, vendors, and any third party acting as an agent of or otherwise on behalf of the University and/or owner.

Classifications:
Public Information: Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.

Controlled Information: Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws.

Confidential Information: Information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. This category also focuses on information that is restricted through certain legal agreements.

Procedure

Classify Data

1. All University data maintained by VPFO IT Services shall be classified as Public, Controlled, or Confidential. The appropriate classification of data is the responsibility of the data owner.
2. All object data types and content shall be identified at the initiation of a project with specific steps included in the project for classifying the resulting data.
3. The data owner (or their designee) shall approve access to data and a written request shall be sent to IT Services. Access changes will be implemented according to IT Services standard Access Control procedures. Access to data shall only be granted upon explicit approval of the data owner.
4. Data access shall be controlled via File System Permissions (NTFS) and Delegated access to Active Directory Objects via Access Control lists. Objects requiring encryption shall use Symantec Desktop Encryption or PGP NetShare folder encryption utilizing centrally managed AES 256 encryption.

5. Where possible, all data files shall be scanned at least yearly for Social Security Numbers. These results will be provided to the data owners for remediation, which includes deletion, redaction, or encryption of actual confidential data.
6. Data classified as *confidential* shall not be stored on user workstations, unencrypted portable devices, or transmitted without being encrypted.

Examples of Data Classifications

Data type	Classification	Security Control
Name	Public	Access Control List (ACL)
UIN alone or with other data	Public	ACL
Budget/Financial	Controlled	ACL
PII	Controlled	ACL
FERPA	Confidential	ACL, Encryption
HIPAA	Confidential	ACL, Encryption
Social Security Numbers	Confidential	ACL, Encryption

Reference: http://assets.system.tamus.edu/files/policy/pdf/SecurityStandards/Data_Classification.pdf