Title: Document Retention and Destruction Policy
Prepared by: Division of Finance and Operations
Administrator: University Compliance Officer
Created: April 1, 2009
Revised: April 5, 2013

Policy Statement

The purpose of this policy is to provide guidelines for how records and documents are to be classified, retained, and destroyed to ensure that data is kept for only the period necessary to conduct business and are destroyed in compliance with federal and state regulations.

This policy applies to data in any form (including paper and electronic documents, e-mail and all correspondence) produced, collected or used by the University, its employees, volunteers, student workers, consultants, or agents during the course of University business.

Responsibilities

All University faculty and staff are responsible for ensuring that data they produce, collect, or use is properly classified, stored and protected and destroyed in accordance with this policy. The Provost and Vice Presidents are responsible for assigning data custodians within their divisions to facilitate this policy. The data custodian must:

- Be familiar with the document retention and destruction policy;
- Develop the department's data management procedures and practices, consistent with this policy;
- Educate faculty and staff within the department in understanding sound data management practices;
- Restrict access to *Protected* and *Sensitive* data and information; and
- Coordinate the destruction of data.

Data custodians should develop and maintain data inventory lists; classify data as *Protected*, *Sensitive*, or *Public;* and properly set a schedule and mode of retaining and destroying data in accordance with

applicable federal and state regulations. Data should not be retained beyond the period that it is needed for business processes or business continuity.

The University Compliance Officer is responsible for collecting data inventory listings from data custodians and monitoring compliance with this policy.

Data Classifications

All data covered by the scope of this policy will be classified as *Protected*, *Sensitive,* or *Public.*

Protected data are paper and electronic data that contain personally identifiable information concerning any individual; is regulated by local, state, or federal privacy regulations or any voluntary industry standards; or best practices concerning protection of personally identifiable information that the University chooses to follow. Any paper or electronic data that contain this information must be classified as *Protected* data by default.

Regulations may include, but are not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Massachusetts General Law Chapter 93H and I
- Payment Card Industry Data Security Standards (PCI DSS)

Examples of *Protected* data must include, but are not limited to:

- Social security numbers
- Credit card and debit card numbers
- Bank account numbers and routing information
- Driver's license numbers and state identification card numbers
- Medical records (including pharmaceutical records)
- CORI (Criminal Offender Record Information) reports
- SORI (Sex Offender Registry information) reports

Sensitive data are any paper and electronic data that are not classified as *Protected* data which the University would not distribute to the general public. Any data is classified as *Sensitive* unless a department gives a more specific classification.

Examples of *Sensitive* data include, but are not limited to:

- Academic advising records
- Student education records
- Admission files, including ACT, SAT and TOEFL scores, and high school and college transcripts and other scholastic records
- Student account data, Perkins and WPI Institute loan information

- Financial assistance application files, student federal work-study information, scholarships and Stafford loan information
- Budgets
- Salary information
- Alumni information

Public data are any paper and electronic data that the University is comfortable distributing to the general public. For department-specific data, this classification comes from the data custodian. If more than one department creates data jointly, the involved departments should jointly classify the data. If they are unable to come to a consensus, the data must be classified as *Sensitive* data. For University-wide data, this classification can only come from the Office of the President, Executive Vice President, the Provost, Registrar, or Human Resources.

Examples of the types of data included as *Public* are:

- Department faculty lists
- Department web and mailing addresses
- Press releases
- WPI web site content

Data Storage and Security

After conducting a review of departmental data to determine its classification in accordance with the Data Classification section above; data custodians shall conduct reviews of the security afforded *Protected* and *Sensitive* data under the department's control to determine that it is safe from unauthorized access or accidental destruction. In all cases, appropriate steps should be taken to provide sufficient physical and electronic security for *Protected* and *Sensitive* data. Those steps include securing paper data in locked file cabinets, or requiring limited and controlled password access to computerized data. In addition, a disaster recovery plan to reconstruct or salvage critical data, in the event of a disaster such as a fire, flood or computer malfunction should be in place.

Data that is electronic will be encrypted and accessed based on the method appropriate to the data classification level. The University's *Password Standard* defines procedures for password protection, password cycling and access controls for electronic data. *Protected* and *Sensitive* data that is paper will be placed in a locked filing cabinet in a limited access space. Access keys and combinations will be limited to just those that are authorized.

Data custodians shall conduct reviews of data in all forms, separating them into appropriate storage media with the objectives of maintaining the data for the appropriate retention period and providing for ease of retrieval when needed. Proper records should be kept to identify the data being stored and their respective retention periods. Backing up and restoring electronic data will be performed according to the Information Technology Department (IT) operating procedures.

Data Destruction and Disposal

Data shall be reviewed by data custodians to verify that the retention period for the data in question has been properly reached. All known audits and audit discrepancies regarding data scheduled for destruction must be settled before the records can be destroyed; all known investigations or court cases involving said data must be resolved before the records can be destroyed. Data custodians will record that the data was destroyed, the date of destruction, and method of destruction. Methods of destruction for specific data types must comply with the IT operating procedures for data destruction.

Electronic documents

The Information Technology Department will assist all University departments with the safe destruction of electronic data. All information in the possession of Information Technology, regardless of classification level or type of media will be securely destroyed prior to redeployment or disposal of computer equipment.

Paper documents

All *Protected* and *Sensitive* data existing in paper form must be disposed of by shredding. All documents should be dropped off in designated containers. Contents will be shredded by a licensed and bonded document destruction company. If a department does not have access to designated shredding containers, the data custodian shall contact the University Compliance Officer to arrange for shredding services.

All *Public* data should be recycled whenever possible.

Questions about this policy

Questions regarding this policy and/or the procedures contained in it should be addressed to the University's Compliance Officer, Michael Curley, ext. 6919 or mjcurley@wpi.edu.