Data Responsibility

Purpose

To ensure that all institutional data vital to the University's business is safely stored and backed up on University approved networked servers.

Policy Statement

All University employees must store University data on University approved networked servers rather than locally on university-owned laptop and desktop computers.

Applies to

All employees (Faculty, Librarians, Administrators, Staff, Graduate Assistants, Student Workers)

Responsibilities

Responsibilities of the Information Technology Division:

- Nightly backup of all data on servers managed by IT (e.g. the W "webhost" drive, the Z "home" drive, the G "department" drive, Webserv, Banner, Blackboard, Moodle, etc.).
- Temporarily provide external hard drives and instructions to University employees to assist in copying data to a new computer.
- Permanently delete all data on external hard drives when not in use.

Responsibilities of all University Employees:

- Ensure all data vital to University business (transaction records, student and employee information, memos, reports, grade books, portfolios, student work, etc.) is only stored on IT managed networked servers (e.g. the W "webhost" drive, the Z "home" drive, the G "department" drive, Webserv, Banner, Blackboard, Moodle, etc.)
- All data stored on a desktop or laptop computer is the responsibility of the individual employee.
- All storage and use of work-related data should be in compliance with the Confidential Data Policy and other related institutional, local, state, and federal policies. Confidential data is defined in the University's Data Classification Standard document.

Title:	Data Responsibility
Approved By:	Patrick Cronin
Approved Date:	April 2011
Date of Last Revision:	July 30, 2013
Policy Category:	Information Technology Division