1.0 Overview
Information assets are assets to the university just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to university operations and the confidentiality of its contents. Once this has been determined, the university can take steps to ensure that data is treated appropriately.

2.0 Purpose
The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

3.0 Scope
The scope of this policy covers all university owned data, stored on university-owned, university-leased, and otherwise university-provided systems and media, regardless of location. Also covered by the policy are hardcopies of university data, such as printouts, faxes, notes, etc. [University owned data should not be stored on non-university owned, leased, etc. systems and media, unless there is explicit written authorization for a short-term need. In such cases, restricted information handling needs to then be applied to the personal media as well.]

4.0 Policy

4.1 Data Classification
Data residing on university systems must be continually evaluated and classified into the following categories:

Level I - Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information. Personal: includes user's personal data, emails, documents, etc.

Level III: Internal: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

Level V - Restricted: any information deemed critical to operations (often this data is internal or confidential as well). Any information deemed proprietary to the business or under state or federal data privacy laws. It is extremely important to identify critical data for security and
backup purposes. See the Restricted Data Policy for more detailed information about how to handle restricted data.

### 4.2 Data Storage
The following guidelines apply to storage of the different types of university data.

#### 4.2.1 Level I - Public
There are no requirements for public or personal information.

#### 4.2.2 Level III - Internal
Internal data must be stored on the network or in the appropriate data system, but does not necessarily need specific backup policies in place around its recovery.

#### 4.2.3 Level V - Restricted
Restricted information must be removed from desks, computer screens, and common areas unless it is currently in use. Restricted information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured. Restricted information should be only be stored on university file servers or in the appropriate university system, and not local hard drives, mobile devices (e.g. smart phones, iPads, etc.) or removable media (e.g. CDs, flash drives, etc.).

Where restricted information has been explicitly authorized to be stored on removable media to support a valid business need, that media must be password protected and encrypted. University owned data should not be stored on non-university owned, leased, etc. systems and media, unless there is explicit written authorization for a short-term need.

Restricted data should be stored on a server or data system that receives frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.

### 4.3 Data Transmission
The following guidelines apply to transmission of the different types of university data.

#### 4.3.1 Level I - Public
There are no requirements for public or personal information.
4.3.2 Level III - Internal
No specific requirements apply to transmission of Internal Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

4.3.3 Level V - Restricted
Restricted data must not be 1) transmitted outside the university network without the use of strong encryption, 2) placed on any removable media without strong encryption (e.g. laptops, flash drives, etc.), 3) left on voicemail systems, either inside or outside the university's network, 4) sent external to the university via postal services without tracking, signature receipt, and delivery confirmation. Restricted data should never be transmitted through non-university systems or to non-university devices without explicit written authorization for a short-term use.

4.4 Data Destruction
The following guidelines apply to the destruction of the different types of university data.

4.4.1 Level I - Public
There are no requirements for public or personal information.

4.4.2 Level III - Internal
There are no requirements for the destruction of Internal Data, though shredding is encouraged.

4.4.3 Level V - Restricted
Restricted data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the university must use the most secure commercially-available methods for data wiping. Alternatively, the university has the option of physically destroying the storage media.

4.4.4 Record Retention
All records are subject to the record retention policy requirements of UW-Platteville, the UW System, and the State of Wisconsin. The university record retention schedules can be
4.5 Applicability of Other Policies
This document is part of the university's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the Assistant Vice Chancellor for Information Technology in consultation with Human Resources and/or the Dean of Students. Violations may result in disciplinary action, which, for students is outlined in Chapter 14 and Chapter 17 of the student conduct agreement and for all individuals may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

6.0 Definitions
Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Backup To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Two-Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History
Revision 1.0, 01/26/2015