1.0 Overview
Restricted data is typically the data that holds the most value to the university and may also be governed by data protection laws. Often, restricted data is valuable to others as well, and thus can carry greater risk in its collection and use than general university data. For these reasons, it is a best practice to dictate security standards that relate specifically to restricted data.

2.0 Purpose
The purpose of this policy is to detail how restricted data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of restricted data, and outlines specific security controls to protect this data.

3.0 Scope
The scope of this policy covers all university-restricted data, regardless of location. Also covered by the policy are hardcopies of university data, such as printouts, faxes, notes, etc.

4.0 Policy

4.1 Treatment of Restricted Data
For clarity, the following sections on storage, transmission, and destruction of restricted data are restated from the Data Classification Policy.

4.1.1 Storage
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. In such cases, restricted information handling needs to then be applied to the personal media as well.
4.1.2 Transmission
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.

4.1.3 Destruction
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 reformating 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.

4.2 Use of Restricted Data
A successful restricted data policy is dependent on the users knowing and adhering to the university's standards involving the treatment of restricted data. The following applies to how users must interact with restricted data:

- Individuals must be advised of any restricted data they have been granted access. Such data must be marked or otherwise designated "Restricted."
- Individuals must only access restricted data to perform his/her job function.
- Individuals must not seek personal benefit, or assist others in seeking personal benefit, from the use of restricted information.
- Individuals must protect any restricted information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is explicitly approved by his or
her supervisor.

- Individuals must report any suspected misuse or unauthorized disclosure of restricted information immediately to his or her supervisor.

- If restricted information is shared with third parties, such as contractors or vendors, a restricted information or non-disclosure agreement must govern the third parties' use of restricted information. Refer to the university's outsourcing policy for additional guidance.

4.3 Security Controls for Restricted Data

Restricted data requires additional security controls in order to ensure its integrity. The university requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for restricted data transmitted external to the university. If restricted data is stored on removable media, laptops or other mobile devices, it must be stored in encrypted form.

- Network Segmentation. Separating restricted data by network segmentation is strongly encouraged.

- Authentication. Strong passwords must be used for access to restricted data.

- Physical Security. Systems that contain restricted data should be reasonably secured. Restricted data stored in hard copies must be secured locked area with restricted access when not in use.

- Printing. When printing restricted data the user should use best efforts to ensure that the information is not viewed by others. Printers that are regularly used for restricted data must be located in secured areas.

- Faxing. When faxing restricted data, users must use cover sheets that inform the recipient that the information is restricted. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the restricted data if it is to be stored. Fax machines that are regularly used for sending and/or receiving restricted data must be located in secured areas.

- Emailing. Restricted data must not be emailed outside the university without the use of strong encryption. Emailing internally should be done on a limited basis with a valid business need. Emails should not be addressed to distribution lists or groups, but to specifically identified individuals to help ensure only those with the need to view restricted information receive it.
• Mailing. If restricted information is sent outside the university, the user must use a service that allows tracking, signature of receipt for the information, and delivery confirmation.

• Discussion. When restricted information is discussed it should be done in non-public places, and where the discussion cannot be overheard.

• Restricted data must be removed from documents unless its inclusion is absolutely necessary.

• Restricted data must never be stored on non-university-provided machines (i.e., home computers).

• If restricted data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

4.4 Examples of Restricted Data
The following list is not intended to be exhaustive, but should provide the university with guidelines on what type of information is typically considered restricted. Restricted data can include:

• Faculty, staff, student, vendor, etc. social security numbers or personal information.

• Medical and healthcare information.

• Electronic Protected Health Information (E PHI).

• Customer data.

• University financial data.

• Product and/or service plans, details, and schematics.

• Network diagrams and security configurations.

• Communications about university legal matters.

• Passwords.

• Bank account information and routing numbers.
• Payroll information

• Credit card information

• Any restricted data held for a third party (be sure to adhere to any restricted data agreement covering such information)

### 4.5 Emergency Access to Data
A procedure for accessing restricted and critical data during an emergency is often a good idea if the university handles information that is integral to the health, well-being, or protection of other persons or entities. If the university maintains this type of data, it should consider establishing such a procedure in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

### 4.6 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.

**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