CES INFORMATION & RISK CLASSIFICATIONS

The University is committed to protecting the privacy of its students, alumni, faculty, and staff as well as protecting the confidentiality, integrity, and availability of information important to the University's mission.

The University classifies its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access. The following table lists the information classifications with the related security risk.

CLASSIFICATION	RISK	EXAMPLES (including, but not limited to . . .)
PUBLIC Information which— -- may, or must, be available to the public and -- has been formally approved for public release	LOW Data and systems are classified as Low Risk if they are not considered to be Moderate, High, or Very High Risk, and: 1. The data is intended for public disclosure 2. The loss of confidentiality, integrity, or availability of the data or system would have ***no adverse*** impact on our mission, safety, finances, or reputation.	 Course catalog information Directory information Press Releases Newsletters
INTERNAL Information which— --is generally accessible within the University to those **with a legitimate university purpose as allowed** by statute, regulations, other legal obligations or mandates or policy; not intended for entities or persons outside the University --may not be specifically restricted by statute, regulations, or other legal obligations or mandates, but -- must be protected against unauthorized use, access, disclosure,	MODERATE Data and systems are classified as Moderate Risk if they are not considered to be High or Very High Risk, and: 1. The data is not generally available to the public 2. The data must be protected for proprietary, ethical, contractual, or privacy reasons. 3. The loss of confidentiality, integrity, or availability of the data or system could have a ***mildly adverse*** impact on our mission, safety, finances, or reputation.	FERPA student records-- -Grades -Courses taken -Schedule -Test Scores -Advising Records -Educational Services received -Student photo -Admissions Employee information contact information— -Home address -email addresses & phone numbers -Demographic attributes University Policies and Procedures Organization charts Library paid subscription electronic resources

acquisition, modification, loss, or deletion.		
CONFIDENTIAL Information which— --requires special handling and controls specific to each work environment that limit access and use -- may not be specifically protected by statute, regulations, or other legal obligations or mandates, but -- is considered by the University's senior management to be private and confidential and as such must be protected against unauthorized use, access, disclosure, acquisition, modification, loss, or deletion. ***Note: This is the default classification of all information not yet classified.***	HIGH Data and systems are classified as High Risk if: 1. Protection of the data may not be required by law/regulation, but must be protected for proprietary, ethical, or privacy reasons. 2. The University is required to self-report to the government and /or provide notice to the individual if the data is inappropriately accessed, or 3. The loss of confidentiality, integrity, or availability of the data or system could have a ***significant adverse*** impact on our mission, safety, finances, or reputation.	Most personal information not publicly available such as salary or performance information and most organization financial information Contracts Non disclosure agreements with vendors/clients Donor contact information

HIGHLY CONFIDENTIAL Information which— --requires the strictest rules of handling and usage --is protected and/or regulated by statutes, policies, or regulations --may also include information for which an Information Trustee has exercised his or her right to restrict access	VERY HIGH Data and systems are classified as Very High Risk if: 1. Protection of the data is required by law/regulation, 2. The University is required to self-report to the government and /or provide notice to the individual if the data is inappropriately accessed, or 3. The loss of confidentiality, integrity, or availability of the data or system could have an ***extreme*** impact on our mission, safety, finances, or reputation.	Directory information for students who have requested that information about them not be released as public information Financial information aggregated above the department level Salary and other personnel data Accounting data and internal financial reports Passwords or credentials that grant access to Internal, Confidential, or Highly Confidential information PINs (Personal Identification Numbers) Birth date combined with the last four digits of SSN and name Social Security number and name Tax ID with name Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) Health Insurance information Medical records related to an individual Bank account or debit card information Electronic or digitized signatures, Private key (digital certificate)