Institutional Data

Office of the Registrar, Office of Student Life, Office of Financial Aid

In general, University Institutional Data is managed according to protocols defined by the following offices (See Table 2):

In some cases, appropriate data classification is guided by state or federal laws that require the University to protect certain types of data (e.g., personally identifiable information such as a social security number or FERPA-protected student education records). In other cases, Data Stewards will consider each security objective using Table 3 as a guide.

As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Office of the CIO for assistance.

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a adverse effect on organizational operations, organizational assets, or individuals.
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.			

The University

a digital signature.