Data Classification and Handling Policy

APPENDIX 2: Safeguarding Information

Managing Private or Public University information in a manner consistent with the criticality of and the requirements for confidentiality associated with the data in any form (electronic, documentary, audio, video, etc.) throughout the entire information lifecycle (from creation through preservation or disposal).

In order to safeguard information:

1. Determine How Much Protection your Information Needs
   The amount/type of protection to be applied to your information depends on an assessment of the need for ***Confidentiality***.

2. Collect Only What is Necessary
   Take reasonable steps to limit the Private Information collected by the unit to that, which is strictly necessary to accomplish a clearly defined institutional purpose.

3. Provide Minimum Necessary Access
   Limit access to files and information to those with a legitimate educational or business interest, ("need to know" or "need to do") based on their institutional responsibilities.

4. Disclose Only the Minimum Information Necessary
   Disclose Private Information only when necessary and only to the extent that such disclosure is consistent with University policy and permitted or required by law.

5. Safeguard Information in Transit
   When transporting or transmitting data electronically or in hard copy, be aware that information is vulnerable to unauthorized access or modification by third parties and take necessary steps to safeguard the information.

6. Secure Physical Equipment and Resources
   Use secure methods to store (e.g., file cabinets, storage vaults, computer hard drives, PDAs), transport (e.g., email, network connections), and process (e.g., PeopleSoft HRIS/PR and Financials, Student System) Private data.

7. Safeguard Information in Storage
   Securely store information, limiting custody/access to as few people as possible to enhance accountability. Document transfers of custody and access.

8. Dispose Information Securely When No Longer Needed
   Use secure methods to dispose of and/or recycle documents, electronic storage media, computers and portable devices when no longer needed or as dictated by published destruction guidelines. (Refer to the KU General Records Retention Schedule.)

9. Stay Informed About Information Risks
   Watch for regular awareness and training information provided by the University.

For more detailed procedural guidance, see the Data Classification and Handling Procedures Guide for the University of Kansas, Lawrence and Edwards Campuses.