GENERAL STATEMENT OF POLICY

Electronic Data are important University assets that must be protected by appropriate safeguards and managed with respect to data stewardship. This policy defines information classifications and assigns responsibility for ensuring information privacy and security at each level of access and control. Information classification, in the context of information security, is the classification of information based on its level of sensitivity and the impact to the University should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what baseline security controls are appropriate for safeguarding that information.

1. All University information shall be categorized in a hierarchical classification level as defined by the data classification guidelines.

2. If information is categorized with multiple classifications, the highest classification amongst the applied classifications shall be applied to that information.

3. Access to university information resources shall be governed by the relationship of the user to the functioning of the university in conjunction with the information classification.

4. University faculty, staff and students shall be educated on the different information classifications and best practices for protecting university information resources.

5. University faculty, staff and students shall be responsible for following governmental regulations and University guidelines for the retention and control of data for which they have access to; violation of which may result in disciplinary action.

6. Electronic media containing university information shall be sanitized or destroyed before disposal or reuse.

The Vice President for Finance and Administration shall be responsible for issuing and maintaining operating procedures to implement this policy.