information may be disclosed to any individual regardless of their relationship to KSU. While data or

information that is classified as public has no restrictions, necessary controls and caution should always be exercised to ensure unauthorized modification does not occur and the integrity of the data remains intact.

Data Classification Chart

2. Data and Access Control

Each of the requirements set forth in this policy are based on the concept of need to know unless data is classified as public. Information must be disclosed only to those individuals who have a legitimate business need, specific authorization or approval for the information.

The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to KSU's systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

Data owners must approve users who will be permitted to gain access to information, and the uses to which this information will be utilized. Requests for access to KSU email, network, or Banner systems must be made to Information Technology. A written or email request must be submitted for all additions or changes to access Information Resources. When an employee changes departments the IT Help Desk must be notified, so access to that department's data can be removed from Information Resources. If access is still required by the employee, it must be approved again by the data owner. When an employee leaves the University, the IT Help Desk must be notified, so access to these Information Resources can be removed. Ex-employees may continue to have access to University email for a limited time, and if a business need requires, with written approval from their Vice President.

All data users must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information regardless of classification.

3. Transmission

Confidential data or files that are to be transmitted over external communication networks, wireless or between computers, must be sent only in encrypted form.

Counice.

Data owners must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access.

Data owners and users must adhere to the Banner Security Audit procedure.

8. Requests for Data or Information

Refer all requests for data or information under the open records law to the General Counsel’s office.

9.

business function supported by the Information Resource or the individual upon whom Data Owners