KENTUCKY STATE UNIVERSITY

KENTUCKY STATE UNIVERSITY
POLICIES AND PROCEDURES

DATA CLASSIFCAITON POLICY

1. Policy

All representatives, affiliates, vendors, contractors or subcontractors of Kentucky State University (KSU) who use, generate, own, come into contact, or have access to, or possession of, KSU internal information are required to familiarize themselves with this data classification policy and to consistently use this policy in their daily KSU business activities or operations. Information is either Public, Confidential, or Restricted information; all three are defined later in this document.

This data classification policy is applicable to all information created, used, or shared at KSU. This includes electronic, hardcopy, and data/information shared verbally or visually.

Data classification, as defined in this document, is based on the concept of need to know, or the principle of least privilege. This term means that information is not disclosed to anyperson who does not have a legitimate and demonstrable business need or does not have specific authorization to receive the information. This privilege, when combined withthe policies defined in this document, will protect the institution's information fromunauthorized disclosure, use, modification, and deletion.

PROCEDURES

1. Classification

KSU data will be classified as followed:

Confidential: This classification applies to the most sensitive data or information that is intended for use strictly within KSU, protected by any confidentiality agreements, or data protected by federal or state law, such as FERPA, HIPPA, GLBA or PCI-DSS. Its unauthorized disclosure could seriously and adversely impact KSU, its customers, its business partners, and its suppliers.

Restricted: This classification applies to less-sensitive business data or information that is intended for use within KSU. By default, all information that is not defined as confidential or public should be treated as restricted. Its unauthorized disclosure could adversely impact KSU, or its customers, suppliers, business partners, or employees, but would not violate law.

Public: This classification applies to data or information that has been approved by KSU administration for release and availability to the general public. This data or 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.

Examples include

electronic mail systems, the Internet, etc. All such transmissions must use a virtual private network, encryption, or similar software as approved by Information Technology. Transmission over personal, or any non-KSU, network is prohibited. When transmitting restricted data over external communication networks, wireless or between computers, encryption is strongly recommended. While data that is classified as public has no transmission restrictions, caution should always be exercised when using or transmitting KSU information.

4. Storage

All KSU employees are responsible for the security and integrity of University information. All such information should be stored on University servers, network storage devices, or University approved Cloud Storage. Data stored on local PC drives is not recommended because such data is not backed up and a failure of a local drive can result in a complete loss of that data. Caution should always be exercised when storing KSU information.

Storage of confidential data on personal or unauthorized computing equipment is prohibited unless approval is received by Information Technology. If approved, then encryption will be required. Storage of credit card information is prohibited on computing equipment.

Storage media containing sensitive (i.e. restricted or confidential) information shall be sanitized completely before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased, it must be destroyed in a manner approved by Information Technology. Please contact Information Technology when needing to dispose or reuse media that contains sensitive data.

5. Documented Backup and Recovery

All confidential data must have a documented backup and recovery procedure.

6. Data Retention

Data retention will adhere to KSU's data retention policy. (Will be a link)

7. Audit Controls

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. Loss of Restricted or Confidential Information

The loss, breach or unauthorized access of any restricted or confidential data or information must be reported immediately to:

- Information Technology
- General Counsel
- Risk Management
- KSU Police Department

Theft or loss of any Information Resource containing any sensitive data must be reported to:

- KSU Police Department
- Information Technology

10. Definitions

Data: Information which is recorded - regardless of form or media – that is used to support the business of the University, whether in an administrative or research capacity. Data may be saved or transmitted in hard copy (printed or written), digital/electronic (video, audio, or photo images) or other formats.

Data Custodian: An employee who is responsible for day-to-day maintenance, backup and recovery, granting access and privileges, and physical security of KSU Information Resources. The Data Custodian shall adhere to information security policies and procedures to manage data or information resources in their care. This is shared a responsibility between Information Technology (backup and recovery) and Data Owners (access and control).

Data Owner or Module Manager: The manager or university official responsible for the business function supported by the Information Resource or the individual upon whom responsibility rests for administering the program using the Information Resources. In addition to following this and other University policies relating to data, the data owner is responsible for training users on the proper handling of data and for the capture, management, and dissemination of data.

Data Ownership: KSU has ownership of all institutional data; data owners, individual units, and/or departments may act as stewards, and may supervise the ways in which certain types of information are used and protected

Data User or User: An individual who is authorized by the Data Owner to access University data as part of their responsibilities or for completion of their role in the University.

Information Resources: Any data and information used by KSU. This includes, but is not limited to procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, share, and transmit information. This may include, but is not limited to, any and all computer printouts, online display devices, mass storage media, and all computer- related activities involving any device capable of receiving email, browsing web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, servers, personal computers, notebook computers, hand-held computers, mobile devices, pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, printers, and hosted services.

2. Entities Affected

- Campus Community
- Information Technology

3. Policy Owner/Interpreting Authority

Executive Vice President of Finance and Administration
Chief Information Technology Officer

4. Related Policies

5. Statutory or Regulatory References