INFORMATION TECHNOLOGY
TITLE: DATA CLASSIFICATION POLICY

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 any person who does not have a legitimate and demonstrable business need or does not have specific authorization to receive the information. This privilege, when combined with the policies defined in this document, will protect the institution's information from unauthorized 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 KSU5Hr: This classification applies to less sensitive business data or inform is intended for use within KSU. By default, all information that is not defined as c or public should be treated as restricted. Its unauthorized disclosure could impact KSU, or its customers, suppliers, business partners, or employees, but violate law.

Public: This classification applies to data or information that has been approve administration for release and availability to the general public. This data or i may be disclosed to any individual regardless of their relationship to KSU. Wh

INFORMATION TECHNOLOGY

TITLE:

INFORMATION TECHNOLOGY
TITLE: DATA CLASSIFICATION POLICY

Data Classification and Handling

	Public	Restricted	Confidential
Description	Data available to the general public.	Less-sensitive business information that is intended for use within the institution.	Data protected by law, regulation, or contract/agreement with KSU.
Examples (not a complete list)	1. Public facing webpages 2. Faculty and Staff Directory 3. Press Releases 4. Marketing brochure 5. Course Catalog	1. Employee data such as the KSU ID, race, ethnicity, and information marked as private. 2. Anonymous Donor Information. 3. Internal reports or memos.	1. Personally Identifiable Information (PII) as defined by KRS 61.878(5) and KRS 61.931(6). 2. Education Records as identified by FERPA. 3. Protected Health Information as defined by HIPPA.
Data Access and Control	There are no access restrictions.	Access is restricted to KSU employees and individuals who have a business need to know.	Access is restricted to those permitted under law, regulation, or KSU polices with a business need to know.
Transmission	There are no encryption requirements.	Encryption not required but strongly recommended.	Must be sent only in encrypted form.
Storage	There are no encryption requirements. Also, necessary controls and caution should always be exercised to ensure unauthorized modification does not occur and the integrity of the data remains intact.	All such information should be stored on University servers, network storage devices, or University approved Cloud Storage. Data owners or custodians will discern the level of protection that is required. If the level is not known, contact Information Technology prior to storage. Necessary controls and caution should always be exercised to ensure unauthorized modification does not occur and the integrity of the data remains intact.	All such information must be stored on University servers, network storage devices, or University approved Cloud Storage. 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.