University of Kentucky
Information Systems Use Policy
(Draft –September 5, 2006)

1.0 Introduction

The University of Kentucky's Information Systems are critical resources and play an integral part in the fulfillment of the University's objectives of teaching, research, and service. The University of Kentucky Information Systems Use Policy provides guidelines for the access, use and protection of these resources.

2.0 Purpose

The purpose of this document is to establish a base-line uniform, campus wide policy and procedures regarding the access, use and protection of all institutional data within the University's custody, including but not limited to confidential, private, personal, or other sensitive information, and to assure compliance with state and federal laws and existing University policies.

This document is intended to establish the minimum requirements for protecting the University from the unauthorized access, modification, destruction or disclosure of confidential, private, personal, or sensitive information. Users should contact the head of their individual college, school and/or department, as each unit may have additional requirements. Other policies that may also affect computer use and access include:

- UKHealthcare Policies
- Policy Governing Access to and Use of University of Kentucky Computing Resources
- University of Kentucky Policy Governing Creation and Maintenance of Materials for the World Wide Web

Of particular note, all units designated as a "Covered Entity" as defined by the Health Insurance Portability and Accountability Act ("HIPAA") and all units dealing with credit cards should verify the security and privacy policies applicable to the User's unit.

3.0 Scope

This policy applies to all University members, including trustees, executive officers, faculty, students, staff, and other individuals employed by the University, those using University resources or facilities, and volunteers and

representatives acting as agents of the University (collectively "University Members").

4.0 Definitions

"Information Systems" includes, but is not limited to, desktop computers, laptop computers, terminals, servers, printers, networks, data, modem banks, online and off-line storage media, wireless hand-held devices, cell phones, access card systems, computer integrated telephony, other technology hardware, databases, data repositories, metadirectories, and related equipment.

"Institutional Data" refers to two general categories of data, public and sensitive information.

- "Public Information" is information that can be freely given to anyone.
- "Sensitive Information" is all other information which is confidential, private, personal, or otherwise sensitive in nature. Sensitive Information includes the following:
  - Personally Identifiable Information (PII) includes an individual's social security number, driver's license or state ID number, financial account numbers with the associated PIN, DNA or any biometric identifier (e.g., a fingerprint, voice print, retina or iris image, or any other unique physical representation). NOTE, while student identification numbers are not Sensitive Information, student identification numbers must never be used to access student education records covered by FERPA, but must always be used in connection with a photo ID or password.
  - Legislatively Protected Data is data which is subject to some government regulation or oversight. This includes, but is not limited to, data as defined under:
    - The Family Educational Rights and Privacy Act (FERPA) – student education records
    - The Health Insurance Portability and Accountability Act (HIPAA) – individually identifiable health information
    - The Gramm-Leach-Bliley Act (GLBA) – personal financial information
  - Other Sensitive Data is data where the unauthorized disclosure could lead to a business, financial and or reputational loss. Examples include all types of intellectual property, research results, potential

development programs, or information protected by a confidentiality agreement.

"Outside Information Systems" includes privately owned Information Systems, which may or may not be managed or maintained by the University (e.g., privately owned desktop or laptop computers).

"Unit" means the functional unit to which an individual is or was assigned or reports. Examples of units include departments, centers, colleges, academic units or administrative units.

"User" includes any person, whether authorized or not, who makes any use of any Information Systems from any location.

5.0 Compliance

To ensure compliance with this Policy and the protection of Institutional Data, the University may access, temporarily suspend, block, or restrict access to its Information Systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Institutional Data or the Information Systems or to protect the University from liability.

6.0 Reporting Violations

All Covered Entities shall report violations in accordance with Health Care Policies. All other alleged violations of the Policies (including but not limited to any unauthorized release, access, use or modifications) shall be reported to the University's Vice President for Information Systems, to the IT administrator responsible for the user's system, and to the Campus or Medical Center IT Security Office for appropriate action.[1] If not already involved, the Vice President of Information Systems shall notify the Office of Legal Counsel and where applicable Human Resources. The Office of Legal Counsel will coordinate any notice appropriate under the circumstances to affected individuals.[2] If the breach involves an apparent violation of law, the Vice President shall also report the breach to law enforcement authorities. The University's Chief Information Security Officer shall coordinate with law enforcement authorities to investigate and respond to such alleged violations.

Reported violations of Policies shall be pursued in accordance with the applicable corrective action procedures for the individual(s) involved, as outlined in the Faculty Handbook, Human Resources Policies and Procedures, the Student Code of Conduct, and other applicable policies and

[1] Users shall also comply with any additional procedures applicable to the user's unit.
[2] While users are strongly discouraged from releasing his or her own Sensitive Information, such a release is not a violation of this policy.

procedures. Violations of this Policy may result in the discipline of the University Member up to and including termination of the relationship with the University. Violations, particularly intentional violations, may also result in criminal prosecution.

7.0 User Access to Sensitive Information

Access to Sensitive Information is granted based on the User's assignment with the University and as determined by the appropriate Administrator or department head, upon consultation with Human Resources, if necessary. Job or assignment functions will determine access to Sensitive Information. Administrators, Department Heads and Human Resources will work to identify:

- Those persons or classes of persons in each department, including faculty, students and staff, who need access to Sensitive Information to carry out their duties;
- The category or categories of Sensitive Information to which physical or computer access is needed;
- Any conditions appropriate to such access, and permissions for copy, removal or transfer for each person or class of persons; and
- The revocation of granted access rights upon change of roles, responsibilities, or termination of employment.

If a User's assignment with the University does not require access to Sensitive Information, then he or she shall not intentionally access such data. If a job or task requires temporary access, the Sensitive Information shall be protected while being used. In no event shall copies of Sensitive Information be maintained beyond the time needed to complete a task or assignment.

When transmitting Sensitive Information in any form (including emails, posting to shared networks, etc.), care should be taken to ensure that the data will only be available to individuals authorized to access it.

8.0 Protecting Institutional Data and Procedures for Protecting Sensitive Information

All University Members shall ensure that Institutional Data are protected from unauthorized release, access, use or modifications. University Members shall observe the requirements for privacy and confidentiality applicable to Sensitive Information, comply with all established requirements for protection and control, and report violations of this policy as described herein.

Units are responsible for ensuring adequate training for authorized users, and adoption of internal controls as needed to meet any specialized security and use requirements.

Sensitive Information stored on University computing resources must be secured and protected using commonly accepted methods. Given the ever evolving nature of information systems, current security guidelines and recommendations can be found on the IT security website.

9.0 Accessing Institutional Data

All Information Systems and Outside Information Systems accessing University host systems shall have security features as defined by IT guidelines that include strong passwords, antivirus software with current updates, and a supported operating system with current patches and updates.

- All remote access to Sensitive Information must utilize network encryption technology (e.g., VPN, SSL). Users must be authorized to activate the VPN connection, run the application and access the data.
- Users should not save Sensitive Information on personal computers unless necessary to perform job functions. If stored on a personal computer, then all reasonable safeguards shall be employed.

Refer to the IT security website for current guidelines.

10.0 Transport of Sensitive Information

Transport of Sensitive Information (e.g., archive tapes, USB drives, laptops, disks, etc.) by individual users shall be protected by all reasonable safeguards. Refer to the IT Security website for current guidelines.