I. PURPOSE

The purpose of this policy is to ensure the protection of the University of Kentucky's (UK) *information assets*[1] from accidental or intentional unauthorized access or damage while also preserving and nurturing the open, information-sharing requirements of tits academic culture.

This policy establishes the UK-wide strategies and responsibilities for ensuring the *confidentiality*, *integrity*, and *availability* of the information assets that are accessed, managed, and/or controlled by UK. Information assets addressed by this policy include all UK data, information, information systems, computers, network devices and documents regardless of their *medium* and regardless of their *location*.

By implementing this policy, UK will:

- Establish a University-wide information security framework to appropriately safeguard access to information resources and services;
- Safeguard against unauthorized access to, use, or sharing of *restricted digital assets* that could potentially result in harm to the University or to members of the University community;
- Safeguard against anticipated threats or hazards to the security of information assets;
- Comply with federal, state, and local law, UK regulations policies, and agreements binding the University that require the University to implement applicable *security safeguards*.

II. APPLICABILITY

This policy is applicable to all University students, faculty and staff and to all others granted use of UK information assets. Every user of any of UK's information assets has some responsibility toward the protection of those assets; some offices and individuals have very specific responsibilities. This policy refers to all UK information assets whether individually-controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, laptops, tablets, personal digital assistants, telephones, smart phones, wireless devices, personal computers, gaming systems, workstations, mainframes, minicomputers, and any associated peripherals and software, regardless of whether used for administration, research, teaching, healthcare or other purposes.

III. POLICY

a. Members of the UK community have individual and shared responsibilities to safeguard the information assets controlled or managed by the University in accordance with federal, state, and local law, University regulations, and agreements binding the University.

b. Each University *unit* shall develop, maintain, and implement an information security program or, in lieu of its own information security plan, shall follow UKAT's information security program as outlined in its **UKAT Information Security Policy & Procedures** documents.

[1] Words that appear in *italics* are defined in the Definitions section.

Units implementing cyber security safeguards, policies and practices that are not explicitly addressed by the **UKAT Information Security Policy & Procedures** shall reference and implement the **SANS Critical Security Controls** and/or the **National Institute of Standards and Technology (NIST)** cyber security policies, procedures, standards and guidelines (i.e., http://csrc.nist.gov/publications/PubsTC.html, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.)

The program shall include (at least) the following:

i. A list of laws and regulations to which the *unit* must comply that are in addition to the laws and regulations listed in the “Confidential” section of the **ISS-6.1 Data Classification Standard**,

ii. A description of any implemented administrative, physical or technical safeguards that are unique to the unit (i.e., safeguards or practices that are exceptions to UKAT recommendations and used to safeguard restricted digital assets), and

iii. An annual program review.

c. Each University unit shall identify and track restricted digital assets under its control. Accordingly, UKAT’s data classification standards and guidelines, **ISS-6.1 Data Classification Standard**, shall be adhered to. Such data classifications are relative to the level of risk that their compromise may pose to the institution

d. Each University unit shall periodically conduct risk assessments around its restricted digital assets. Risk assessments will prioritize risks and recommend appropriate mitigation strategies.

e. Each University unit shall report and manage information security incidents in accordance with established policies and guidelines (i.e., the UK Information Security Incident Reporting Policy.)

f. Each University unit shall implement safeguards that are appropriate to digital asset *sensitivity*, *criticality*, and the level of risk identified in the risk assessment process.

g. In lieu of policies, procedures, standards and guidelines that have been fully vetted and approved by University technology governance committees (per UK Administrative Regulation 10:2), draft policies, procedures, standards and guidelines that have been approved by either the University CISO or the unit’s chief administrative officer shall suffice as valid and appropriate.

IV. RESPONSIBILITIES FOR IMPLEMENTATION

University Deans and Directors are responsible for implementing and ensuring compliance with this policy. Responsibilities include:

a. Communicating this policy to their community and ensuring appropriate education and training;

b. Designating individuals to unit information security roles, ensuring they are properly trained, and ensuring their ongoing participation in University-wide information security activities;

c. Ensuring the implementation of information security plans within their units;
d. Ensuring unit collaboration on the implementation of the University-wide Information Security Program.

The Chief Information Security Officer is responsible for:

a. Directing and coordinating the University-wide Information Security Program;

b. Developing, vetting, gaining approval for, and maintaining this and all supporting information security policies, procedures, standards, and guidelines.

c. Determining unit-level compliance with this policy;

d. Providing a focal point for oversight of serious security incidents as indicated in the UK Information Security Incident Reporting Policy;

e. Establishing security metrics, tracking the progress of the Information Security Program and providing a University-wide risk profile;

f. Assisting units in fulfilling their information security requirements; and

g. Annually reviewing/assessing the UK information security program and making appropriate recommendations and changes.

V. DEFINITIONS *(not complete)*

AFFILIATES refers to organizational units that are either managed in whole or in part by the University of Kentucky, an auxiliary unit of UKAVAILABILITY refers to the level of assurance that authorized users have access to information assets when required.

CONFIDENTIALITY refers to the level of assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes.

CRITICALITY refers to the relative importance of the information asset to the mission of the University and reflects the degree to which the information requires safeguarding to ensure it is not accidentally or maliciously altered or destroyed.

INFORMATION ASSET refers to data, information, system, computer, network device, document, contractual agreement or any other component of the university infrastructure regardless of its medium or location which is used by UK employees and *affiliates* to help the University accomplish its *Mission*.

INTEGRITY refers to the assurance that information is not accidentally or maliciously altered or destroyed.

SECURITY SAFEGUARDS refer to protective measures prescribed to meet security requirements (i.e., confidentiality, integrity, availability) specified for an information asset or environment. Also called security controls or countermeasures.

SENSITIVE INFORMATION refers to information whose unauthorized disclosure may have serious adverse effect on the University’s reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive.

SENSITIVITY refers to the degree to which information requires protection to ensure it is not exposed to unauthorized users.

UNIT refers to any organization across the University such as a school, college, department, or central office. The Health System as well as the Flint and Dearborn campuses are considered University units.

VI. REFERENCES

VII. REVISION HISTORY

Date	Description	Primary Author
12/18/14	Initial draft developed	M. Carr