I. PURPOSE

The purpose of this policy is to ensure the proper handling, investigation, and response to information security breaches of personal information at UK. The University will make every effort to prevent a breach of UK information systems or physical hard-copies from occurring; however, in the event of such a breach, the University must work quickly and diligently to detect, internally notify, and remediate.

It is incumbent upon UK to:

- Investigate alleged or suspected unauthorized access or inadvertent sharing of personally identifiable information at the University of Kentucky;
- Engage appropriate Information Security Incident Response Team(s) (ISIRT) for investigations, remediation, and after-action reviews;
- Determine whether a breach of protected personal information has occurred; and
- If necessary, make the required notifications to state officials and affected individuals.

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 applies to all UK information assets whether individually-controlled, stand-alone, shared, networked or processed/stored by a third party at UK's behest.

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. Suspected or alleged unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of personal information (hereafter referred to as an "Incident") shall be reported immediately through the:

   i. **UK Security Breach Reporting Line** (by calling (859) 218-3904);
   ii. **UKHC Corporate Compliance Office**; or
   iii. **UK HealthCare ITS Help Desk** (by calling (859) 323-8586).

b. Suspected or alleged Incidents involving protected health information or personal information containing protected health information shall be reported to UKHC Corporate Compliance and handled in accordance with the UK HealthCare Privacy Investigations and Breach Notification Policy, A06-100, www.hosp.uky.edu/policies/viewpolicy.asp?PolicyManual=10&PolicyID=3740.

c. Upon notification of such Incidents, the appropriate Incident Response Team shall be contacted. The Incident Response Team or Chief Information Security Officer shall contact the UK Security Breach Notification Committee when necessary for further processing.

d. The UK Security Breach Notification Committee may consist of personnel from the following offices:

i. UK Analytics and Technologies;
ii. UKHC Information Technology and Security;
iii. Office of Legal Counsel;
iv. Risk Management;
v. Public Relations;
vi. UKHC Corporate Compliance;
vii. Human Resources; or
viii. Other offices/departments as necessary.

IV. RESPONSIBILITIES FOR IMPLEMENTATION

The UK Security Breach Notification Committee or designee shall:

a. Investigate and respond to inquiries and complaints made through the methods above, including telephone calls, e-mail, written notice, in person, referral from management, customer service or through other means;

b. Investigate and monitor compliance with government regulations and internal policies that relate to an individual's personal information;

c. Recommend corrective and recovery actions and system improvements in areas that present personal information risks on a monthly basis;

d. Upon determination or notification of a security breach relating to personal information collected, maintained, or stored by the University of Kentucky or a nonaffiliated third party on behalf of the University of Kentucky:

a. Within seventy-two (72) hours, notify the appropriate state officials, in writing,

b. Conduct a security breach investigation to determine whether the security breach has resulted in or is reasonably likely to result in misuse of personal information.

c. If misuse has occurred or is likely to occur:

i. Within forty eight (48) hours of completion of the investigation, notify the appropriate state officials and the Commissioner of the Department for Libraries and Archives, in writing;

ii. Within thirty-five (35) days of the aforementioned notifications to the appropriate state officers, notify all affected individuals; and

iii. If the number of affected individuals exceeds one thousand (1000), seven (7) days prior to the individuals being notified, notify the Council on Postsecondary Education and all consumer credit reporting agencies on the list

maintained by the Office of the Attorney General (i.e., credit reporting agencies that compile and maintain files on consumers as defined in 15 USC § 1681a(p) on the timing, distribution and content of the notices sent to the affected individuals.)

iv. The notifications to affected individuals may be delayed beyond the thirty-five (35) day timeframe if:

1. A written request to delay the notification due to a criminal investigation is received from a law enforcement agency; or
2. It is determined that data integrity cannot be restored within the timeframe and the delay is approved in writing by the Office of the Attorney General. Once integrity is restored, notification shall be made immediately.

d. If misuse of personal information has not occurred or is not reasonably likely to occur, notify the appropriate state officials that misuse of personal information has not occurred and maintain records reflecting the basis for its decision for the retention period of six (6) years.

The Chief Information Security Officer is responsible for:

a. Directing and coordinating the UK Security Breach Notification Committee;
b. Activating the Information Security Incident Response Team(s);
c. Identifying and recommending resource appropriations, when necessary, to the UK Security Breach Notification Committee;
d. Determining unit-level compliance with this policy; and
e. Providing a focal point for the oversight of serious security incidents.

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 UK.

APPROPRIATE STATE OFFICIALS refers to:

- Commissioner of the Kentucky State Police;
- Auditor of Public Accounts;
- Attorney General; and
- President of the Council on Postsecondary Education

AVAILABILITY 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.

ENCRYPTION refers to the conversion of data using technology that meets or exceeds the level adopted by the National Institute of Standards & Technology (NIST) as part of the Federal Information Procession Standards (FIPS) and renders the data indecipherable without the associated cryptographic key to decipher the data.

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.

NONAFFILIATED THIRD-PARTY refers to any entity that (a) has a contract or agreement with the University of Kentucky and (b) receives personal information from the University of Kentucky pursuant to the contract or agreement.

PERSONAL INFORMATION refers to an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) of more of the following data elements:

- An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
- A social Security number;
- A taxpayer identification number that incorporates a Social Security number;

- A driver's license number, state identification card number, or other individual identification number issued by any agency;
- A passport number or other identification number issued by the United States government; or
- Individually identifiable health information as defined in 45 C.F.R. sec. 160.103 except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

SECURITY BREACH refers to:

(1) The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or the agency *or nonaffiliated third party* reasonably believes may compromise the security, *confidentiality*, or *integrity* of *personal information* and result in the likelihood of harm to one (1) or more individuals; or

(2) The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing *personal information* along with the confidential process or key to unencrypt the records or data that compromises or the agency or *nonaffiliated third party* reasonably believes may compromise the security, *confidentiality*, or *integrity* of *personal* information and result in the likelihood of harm to one (1) or more individuals.

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
12/19/14	Initial draft developed	M. Carr