I. PURPOSE

Threats to the confidentiality, integrity, and availability of University data and resources may come from third-parties or the workforce. While preventive measures lessen the threat, they cannot eliminate it. The University of Kentucky must be able to detect, respond to, report and learn from information security incidents. This policy defines a consistent means to deal with information security incidents. It is the responsibility of every employee to report an incident.

By implementing this policy, UK will:

- Investigate alleged or suspected security incidents at the University of Kentucky;
- Implement one or more Information Security Incident Response Teams (ISIRT) for investigation, remediation, recovery, and after-action review;
- Conduct an annual exercise of the incident response procedures; and
- Document and maintain records of those exercises.

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. The University shall establish and implement an incident response program that meets the following requirements:

   i. Identifies a point of contact for information security incidents;
   ii. Includes an Information Security Incident Response Team (ISIRT); and
   iii. Includes an incident response plan.

b. All information security incidents, suspected or confirmed, shall be promptly reported through established reporting mechanisms.

c. The University shall develop a plan for the handling and processing of security incidents. This plan shall address the following phases of handling:

   i. Identification of incident(s);
   ii. Analysis of incident(s), including forensics;
iii. Containment of incident(s);
iv. Eradication & remediation of vulnerabilities;
v. Recovery of operations after incident(s); and
vi. Follow-up assessment.

d. Recording and documenting steps shall be taken during each phase and evidence shall be collected and secured. These items are to be used for the analysis of security incidents, disciplinary action handled, or to achieve admissibility of evidence in a court of law.

e. The incident response plan shall be reviewed on an annual basis for accuracy and to keep pace with technology changes.

IV. RESPONSIBILITIES FOR IMPLEMENTATION

The Chief Information Security Officer is responsible for:

a. Directing and coordinating the Information Security Incident Response Team(s) (ISIRT);
b. Activating the ISIRT team(s) as necessary to response to security incidents;
c. Pulling in people, resources, and subject matter experts to serve on ISIRTs:
d. Determining unit-level compliance with this policy; and
e. Ensuring that at least annual exercises of the procedures herein are performed and documented.
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.

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.

EVENT refers to an observable change to the normal behavior of a system, environment, process, workflow, or person.

INCIDENT RESPONSE refers to the process of formulating teams for responding, investigating, remediating, recovering, and conducting a follow-up review to an information security incident.

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.

INFORMATION SECURITY INCIDENT refers to any real or suspected threat to the confidentiality, integrity, or availability of University of Kentucky data, information assets, or resources.

INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT) refers to a capability set up for the purpose of investigating and determining response to information security incidents.

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

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.

VULNERABILITY refers to a weakness in a process, system, application, or network that is subject to exploitation or misuse.

VI. REFERENCES

VII. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Primary Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/07/15</td>
<td>Initial draft developed</td>
<td>D. Merida</td>
</tr>
</tbody>
</table>