TITLE: INFORMATION SECURITY POLICY

PUPROSE

The purpose of this policy is to communicate to the security measures required to ensure the appropriate protection and safeguarding of Kentucky State University's Information Technology resources and systems from unauthorized access and misuse.

SCOPE

This policy and all implementing standards and procedures applies to all KSU students, faculty, staff, Board of Regent members, and all others who use, have access to, store, transmit or oversee KSU information technology resources. This applies to access of any KSU information resource from any device.

POLICY

It is the policy of KSU to implement security measures to prevent unauthorized access or destruction of Information Technology resources and systems. The security measures will ensure the confidentially, integrity and availability of Information Technology resources and systems. By implementing this policy, KSU will address:

- Acceptable Use
- Awareness and Training
- Access Control
- Audit and Accountability
- Data Classification
- Business Continuity and Disaster Recovery
- Incident Response
- Enforcement

Every user of any of KSU's Information Technology resource and/or systems bears responsibility in the protection technology resources.

KSU will adhere to federal, state laws, rules, regulations, policies and procedures governing the confidentiality and protection of data.

INCIDENT REPORTING

Any member of the KSU community who suspects or becomes aware of an Information Security Incident must report the incident immediately by:

1. Contacting the IT Help Desk or Chief Information Officer by phone (preferred), e-mail or in person.
2. Contacting the department supervisor, who must contact the CIO immediately.

3. If the department supervisor is not available, then the individual must contact the division Vice President, who must contact the CIO immediately.

Suspected violations of this policy should be reported to the Chief Information Officer.

ENFORCEMENT

Any individual who violates this policy may result in disciplinary action including but not limited to termination, loss of data access privileges, administrative sanctions, and personal civil and criminal liability.

Any employee or student who interferes with or refuses to cooperate in the investigation of a violation of this policy may be subject to disciplinary action including but not limited to termination, loss of data access privileges, administrative sanctions, and personal civil and criminal liability.

DEFINITIONS

Information Security Incident: An actual or suspected event such as a violation of computer security policies, acceptable use policies, or standard security practices. These events may adversely affect the security of KSU's information resources or systems. Examples include:

- Web site defacement
- Theft or loss of a computing device that may contain Personal Identifiable Information (PII) whether or not such device is owned by KSU
- Unauthorized access to data
- Computer infected with malware (examples include a worm, virus, Trojan Horse, or botnet)
- Reconnaissance activities (such as network or vulnerability scanning, or hacking/penetration testing)
- Data Breach
- Misuse of Information Resources or Systems
- Denial of Service attacks
- Security vulnerabilities (such as an un-patched or vulnerable systems)

Information Technology Resource is defined as any data, information or system used by KSU. This includes, but is not limited to procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, share, and transmit information. This may include, but is not limited to, any and all computer printouts, online display devices, mass storage media, and all computer related activities involving any device capable of receiving email, browsing web sites, or otherwise capable of receiving, storing, managing, or

transmitting data including, but not limited to, servers, personal computers, notebook computers, hand-held computers, mobile devices, pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, printers, and hosted services.

Information Technology System is defined as any electronic system that processes, stores or transmits information.

Personal Identifiable Information (PII): Per KRS 365.732 this is defined as individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account