KENTUCKY STATE UNIVERSITY

KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

UNIVERSITY DATA POLICY

1. Policy

PURPOSE: To establish policies for the University with respect to data security, access and review along with data backups and disaster recovery.

OBJECTIVE: To minimize the loss of University data.

POLICY:

I. Data Security

a. Passwords should be treated as confidential information and must not be shared.
b. Password protected screen savers are mandated on all University owned computers set to a maximum time out of 15 minutes.
c. Employees are responsible for the security and integrity of University information and all such information should be stored on University servers, Network storage devices or University approved Cloud Storage and is NOT to be stored on local PC drives (c; drive, d: drive), USB attached storage (also known as – jump drives, flash drives, portable hard drives), CD/DVD or any other device. Local data is NOT backed up. A failure of a local drive can result in a complete loss of that data.
d. All employees must encryption all files that have personally identifiable information (Social security, number, date of birth, driver's license number etc.). For Microsoft products go to "File" then "Protect Document" and follow instructions.
e. If an application does not have encryption capabilities it is not allowed to be used with personally identifiable information.
f. No personally identifiable information is allowed in the body of an email.
g. Encrypted files with personally identifiable information are allowed to be emailed, but the email must NOT contain the encryption key.
h. The encryption key may be communicated over the phone or in a separate email.
i. Network passwords are enforced to change every 180 days.
j. All requests to reset passwords are performed by the Information Technology Helpdesk or online. Users must give proof of identity prior to the password being reset. Proof of identity includes KSU ID number, show ID if in person or other information known only to the person.
k. All backups of personally identifiable information must be encrypted.

II. Data Access and Review

a. Information Technology will serve as the custodian of University data.
b. Module managers/department heads will serve as data owners.

c. Data Owners must approve access to their data. User will submit completed access request forms from the Intranet with approval for access to the IT Help Desk.
d. IT will fulfill all completed and approved forms, incomplete forms will be returned to owners
e. Requestor will be notified via email when completed.
f. A request form must be submitted for all additions or changes to access.
g. When and employee changes departments the IT Help Desk must be notified, so access to that departments data can be removed. If access is still required by the employee it must be approved again by the data owner.
h. When and employee leaves the University the IT Helpdesk must be notified, so access to University systems can be removed.
i. Ex-employees may continue to have access to University email for a limited time with approval from their Vice President.
j. Risk Management with assistance from IT will periodically send out security reports to all data owners for review.
k. Periodic audit reviews will be conducted by Risk Management Department with assistance from IT.

III. Data Backup

1. Information Technology as custodians of data will perform daily backups and store tapes in a fireproof safe.
2. The IT department will maintain a weekly archive of backup tapes in a secure offsite storage location.
3. The IT department will maintain a six-month archive of data tapes in a secure offsite storage location.
4. The IT department will maintain an annual archive of data tapes in a secure offsite storage location.

IV. Disaster Recovery

a. The IT department will maintain a Recovery Point Objective within one day in the event of a disaster.
b. The IT department will maintain a Recovery Time Objective within two weeks, to rebuild infrastructure and to get essential systems functioning in the event of a disaster.
c. The IT department along with the Payroll depart will maintain a process to transmitting a payroll file within 3 days in the event of a disaster.

Questions regarding this policy should be directed to the Information Technology Help Desk at helpdesk@kysu.edu.

2. Entities Affected

- Academic Affairs

3. Policy Owner/Interpreting Authority

Provost/Vice President for Academic Affairs

4. Related Policies

5. Statutory or Regulatory References