

Education and Workforce Development Cabinet
POLICY/PROCEDURE

Effective Date: September 1, 2006
Revision Date: August 24, 2006

Subject: Digital data access

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) for end-user digital data access.

Scope: This policy applies to all EDU employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on an EDU maintained server or workstation.

Policy/Procedure Maintenance Responsibility: The EDU Security Audit Group (SAG) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM.

Applicability: All EDU employees and contractors shall adhere to the following policy.

Responsibility for Compliance

Each Department is responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, intentional misuse and/or inappropriate use may result in disciplinary action pursuant to KRS 18A up to and including dismissal. It is also each Department's responsibility to enforce and manage this policy.

Overview

The purpose of this policy is to define the requirements to safeguard data/sensitive data on portable devices and portable electronic storage media on or off the Commonwealth of Kentucky "State" premises, and the procedures to be followed.

This policy applies to all agencies and organizations within the Education Cabinet that create, store or access data/sensitive data.

This policy defines minimum requirements; agencies may adopt more stringent requirements.

Definitions:

Data: Refers to data that is collected by the agencies and organizations with the Education Cabinet and stored on State devices.

Sensitive Data: Refers to data that is held confidentially, and if compromised may cause harm to individual citizens or create a liability for the State. Sensitive Data is considered to be in electronic form. Examples include, but are not limited to:

1. Confidential employee information
2. Confidential citizen/individual information
3. HIPAA-regulated information
4. FERPA-regulated information
5. Criminal justice information
6. Driver's license numbers
7. Social Security Numbers
8. Trade secrets
9. Account Numbers
10. Credit or Debit Card Numbers
11. Information in combination with any required security codes, access codes, or password that would allow access to individual accounts.
12. Application program code

Portable Devices: Electronic computing and communications devices designed for mobility, including laptop, desktop, in-vehicle personal computers, personal data assistants (PDAs), cellular devices (cell phones, Blackberries) and other devices that have the ability to store data electronically.

Portable Electronic Storage Media (Portable Storage): Includes floppy disks, CDs, DVD, optical platters, USB Drives or flash memory drives, backup tapes, external hard drives and other electronic storage media that provide portability or mobility of data.

Secured Storage Environment: Data storage devices and support systems, such as direct attached server storage and Storage Area Network devices, managed by State personnel or provided explicitly under contract, and are secured by physical and logical means consistent with data storage best practices and recommendations.

Requirements/Procedure:

A. Requirements

Storage of Data/Sensitive Data is restricted:

1. Agencies shall collect, store and use Data/Sensitive Data based on business requirements.
2. Access shall be based on business requirement and limited solely to users authorized by

management.

Data/Sensitive Data:

1. Not copied or removed from Secured Storage Environments unless there is a business requirement and management approval.
2. Not used or stored outside of State offices unless there is a business requirement approved by management.
3. Not be transmitted via non State-owned networks unless approved transmission protocols and encryption techniques are utilized.
4. Not be transported outside of the United States on portable devices and portable storage.
5. Only be stored on state-owned portable devices and portable storage if there is a business requirement and is approved by management.
6. Sensitive data must be encrypted when taken off state premises on portable devices and portable storage.
7. Not be transferred to non State-owned portable devices or portable storage unless there is a business requirement and is approved by management.

Each agency/organization shall:

1. Maintain a documented audit trail (including a date/time record of significant changes) and inventory of:
 - a. Who has what Data/Sensitive Data
 - b. What is the business requirement with management approval
 - c. What portable devices or storage are used.

Procedural Issues

All Data/Sensitive Data to be taken offsite requests must be submitted for approval using form EDU_F03.

Review Cycle:

Annually

Timeline:

Effective Date: September 1, 2006

Revision Date: August 24, 2006

Review Date: May 15, 2012

DTS Standards

Cross Reference: EDU Security Request Change Report Form EDU_F03

Acknowledgement of Policy

I _____ (**print name**) have read and understand the conditions of the Digital Data Access Policy EDU-13.

Signature: _____

Date: _____

Management signature: _____

Date: _____