

**Policy Number:** EDU-22  
**Subject:** Inter Agency Digital Data Access and Sharing

**Education and Workforce Development Cabinet**  
**POLICY/PROCEDURE**

**Effective Date:** August 1, 2009

**Revision Date:** July 30, 2009

**Subject:** Inter\Intra agency Digital data sharing

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

**Scope:** This policy applies to all contracted agencies both State and Federal, including all persons providing contractor services, who use, process, store or share 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, and that 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 being accessed and shared on the Commonwealth of Kentucky “State” premises, and the procedures to be followed.

This policy applies to all contracted agencies both Federal and State that create, store or access data or sensitive data and shares the records.

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

## **Definitions:**

**Data:** Refers to data that is collected by the agencies and organizations within the Education and Workforce Development 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

Sharing of data by:

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.

Transmission of secured data by either Local Area Network (LAN) or Wide Area Network (WAN) must be consistent with data sharing best practices and recommendations.

**Requirements/Procedure:**

A. Requirements

Storage and sharing of Data/Sensitive Data is restricted as follows:

1. Agencies shall collect, store, use and share data based on business requirements.
2. Inter/Intra agency access and sharing of data shall be based on business requirement and limited solely to users authorized by management.

Data/Sensitive Data:

1. Shall not be copied, removed, shared or transmitted from Secured Storage Environments unless there is a business requirement and management approval.
2. Shall not be used, stored, shared or transmitted outside of State offices unless there is a business requirement approved by management.
3. Shall not be transmitted via non State-owned networks unless approved transmission protocols and encryption techniques are utilized.
4. Sensitive data must be encrypted when transmitted off state premises.
5. Shall not be transmitted to non State Agencies 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 Who has what access to the Data/Sensitive Data
2. This policy applies to all contracted agencies both Federal and State that create, store, or access data or sensitive data and shares the records.

**Procedural Issues**

Shared data by contracted agencies both Federal and State must be submitted for approval using form EDU\_F03.

**Review Cycle:**

Annually

**Timeline:**

Revision Date: July 30, 2009

Review Date: November 30, 2011

Effective Date: August 1, 2009

**DTS Standards**

Cross Reference: Education and Workforce Development Cabinet Security Request Change Report Form EDU\_F03

**Acknowledgement of Policy**

I \_\_\_\_\_ (print name) have read and understand the conditions of the Digital Data Access and Sharing Policy EDU-22.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Management signature: \_\_\_\_\_

Date: \_\_\_\_\_