

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

Effective Date: March 1, 2008
Revision Date: January 25, 2008

Subject: Personal Information Policy

Policy: This policy supports the Education Cabinet (EDU)

Scope: This policy applies to all Education and Workforce Development Cabinet (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 outline measure so that agencies can protect any sensitive data they may send electronically (email, internet, intranet, file transfer, etc.). "Personal Identifiable Information (PII)" PII does not include publicly available information that is lawfully made available to the general public from Federal, State, or Local Government records,

Definitions: Personal Identifiable Information (PII): means an individual's first name or first initial and last name, or birth date, in combination with any of the following identifying information of the individual including but not limited to:

1. Social security number;

2. National Identification number;
3. Tax identification number;
4. driver's license number;
5. Personal identification number;
6. Fingerprints, face, or handwriting or other biometric data;
7. Digital identity;
8. Mother's maiden name;
9. Credit card number;
10. Debit card number;
11. Medical identification number or information;
12. Account Number;
13. Password;
14. Code;

Cabinet Policy: The purpose of this document is to provide guidance on the use of PII being transmitted electronically. With the current climate regarding Identity Theft, it is imperative that state employees take appropriate precautions when transmitting data electronically.

State employees should be aware that Management and other authorized staff have the right to access any material on your computer at any time or in your email. Employees should not consider electronic communication, storage or access to be private if it is created for, stored at work or on state owned equipment.

Numerous Privacy Laws have been enacted that makes it a crime to "knowingly, intentionally, or recklessly discloses PII". These laws include the Privacy Act of 1974, The Health Information Portability and Accountability Act (HIPPA), Family Education Rights and Privacy Act (FERPA) and the Social Security Number Privacy and Identity Theft Prevention Act of 2004. Employees may be prosecuted if they inadvertently or recklessly allow PII to be disclosed or obtained by unauthorized recipients.

Procedure:

If sensitive information is sent via, the internet, intranet, email or other unsecured media transmission service, the information must be sent encrypted. Current encryption solutions include Virtual Private Networking (VPN), Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), secure FTP (SFTP), Secure Shell (SSH), and Entrust for encrypting e-mails.

Procedural Issues

Any information with PII transmitted electronically within or outside of the State

network will be secured (encrypted). Sensitive Commonwealth of Kentucky information must not be faxed via un-trusted intermediaries like hotel staff, rented mailbox store staff, etc.

Review Cycle:

Annually

Timeline:

Effective Date: March 1, 2008

Revision Date: January 25, 2008

Review Date: May 11, 2012

Enterprise Security and Policies

Cross Reference:

DTS Standards

Cross Reference:

EDU-01 Internet and Email Acceptable Usage

EDU-12 Network Services - Data Storage

EDU-13 Digital Data Storage-Transport