

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

STATEMENT OF AUTHORITY

1. The Finance and Administration Cabinet’s Standard Procedures Manual establishes standard mandatory internal procedures cabinet-wide. These procedures are established in accordance with the Secretary’s statutory authority under KRS 42.014 and KRS 12.270 to establish the internal organization and functions of the Cabinet as necessary to perform the duties effectively.
2. The Standard Procedures Manual may only be revised in accordance with the process outlined in Standard Procedure #1.1 entitled: “Finance Standard Procedures and Manual”.

I. PURPOSE

The Finance and Administration Cabinet (Cabinet) is responsible for the administration of various types of data including confidential information received from the public, state and federal agencies as well as from state employees. The purpose of this policy is to establish guidelines to which all Cabinet employees will be aware of how to handle and collect confidential information that is owned by or entrusted to this Cabinet whether the information is electronic, physical documents or in any other format.

II. DEFINITIONS

“Confidential information” means any information not exempted in specific legislation and identified as personal, sensitive or confidential such as personally identifiable information, individually identifiable health information, education records and non-public information as specified in all applicable federal or state laws.

“Confidentiality” means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

“Education records” means those records that are (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.

“Individually identifiable health information (IIHI)” means information that is a subset of health information, including demographic information collected from an individual, and includes (1) information created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past,

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is reasonable basis to believe the information can be used to identify the individual.

“Non-public information” means information not known by the public and is protected from disclosure by federal and state law and regulations.

“Personally identifiable information (PII)” means any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number (SSN), date and place of birth, mother’s maiden name or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information. PII includes, but is not limited to, any of the following information related to a person:

- Name, such as full name, maiden name, mother’s maiden name, alias, login name, screen name, nickname or handle
- Personal identification number, such as SSN, passport number, vehicle registration plate number, driver’s license number, taxpayer identification number, bank account numbers or credit or debit card numbers
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or identifying characteristics), fingerprints, handwriting or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, birth place, race, religion, weight, activities, geographical indicators, employment information, performance evaluations, medical information, education information, financial information, income tax records, IP address).

III. PROCEDURE

A. Identify Location of Confidential Information

1. Each organizational unit within the Cabinet is required to identify and inventory where confidential information is received, processed, transmitted or stored for its area of operations. A list of individuals with access to each of these areas should be

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

maintained and kept current. Examples of locations to consider are listed below:

- a. Local storage device: Includes hard drives of servers, desktops and laptops.
- b. Miscellaneous: Includes emails, electronic documents and spreadsheets.
- c. Physical document storage environment: Includes containers, workstations, offices, filing cabinets, safes and drawers.
- d. Portable Electronic Devices: Electronic computing and communication devices designed for mobility including personal data assistants (PDAs), tablets, cellular devices and other devices that provide mobility and have the ability to store data electronically.
- e. Portable Electronic Storage Media (Portable Storage): Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes and other electronic storage media or devices that provide portability or mobility of data.
- f. Printed media: Includes forms, reports, books, printed information, ledgers, microfilm and microfiche.
- g. Remote storage device: Includes shared/mapped drive, external tape drive, network attached storage (NAS), storage area network (SAN) and cloud servers.

B. Storage of Confidential Information

1. The Cabinet will take measures to protect confidential information against unauthorized access, unauthorized use, loss or damage.
 - a. Individuals
 1. Confidential records shall be kept locked up at all times when they are not actually being used. That is, they shall be kept in locked workstation, locked cabinets or in locked rooms after business hours and whenever the person using them is not present. (See [CIO-072: Identity and Access Management Policy](#))
 2. If confidential records are maintained in electronic form on removable media, the medium on which the files are stored (e.g., CD's, thumb drives/flash drives and removable hard drives) shall be kept in locked containers supplemented by office door locks. If maintained on a computer, access shall

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

be secured by all reasonably available means (including keyboard locks, passwords and encryption).

3. Unencrypted storage of confidential data on portable devices and/or portable media is strictly prohibited. (See [CIO-092 Media Protection Policy](#))
4. In all cases, every attempt must be made to assess the impact of storing, and to mitigate the risk to, confidential data on all mobile devices. If confidential data is placed on any mobile devices, that device shall have automatic full encryption that does not require user intervention nor allow user choice to implement. Employees must not redirect confidential or privileged State data to a non-State owned computing device or PDA without proper authorization. (See [Enterprise Standards and Approved Products 5100: Encryption](#))
5. UserIDs must be individually owned in order to maintain accountability. Each UserID must be used by only a single individual who is responsible for every action initiated by that account. UserIDs, passwords or other forms of electronic authentication involving access to confidential information shall not be shared or disclosed to other individuals. (See [CIO-072: Identity and Access Management Policy](#))
6. Label information system media and output containing confidential information to indicate how it should be distributed and handled. Examples of labeling are coversheets on printouts and paper labels on digital media.
7. Employees should contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource containing confidential information, or if questions arise regarding acceptable or unacceptable uses.
8. Position monitors and printers so that others cannot see or obtain confidential or sensitive data.
9. Confidential information shall not be transmitted by email unless by means of an approved COT secured system (encryption). Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI) or other sensitive data (i.e., credit card numbers, calling card numbers, logon passwords, health information or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

10. Fax machines that are used to receive and/or transmit confidential information shall not be located in an area where documents can be screened from the casual viewer. When faxing information, it shall include a coversheet clearly identifying the recipient or addressee and his/her contact information along with a confidential information statement outlining steps required to be taken if the information is received by an unauthorized individual. This area shall be locked after hours or when not attended by authorized individuals.
11. Confidential information shall not be removed from the worksite unless authorized as necessary for work-related purposes. Protect digital media, non-digital media and mobile devices containing confidential information that are transported outside the organization's controlled areas by encrypting the stored information and/or locking the media in a container. Adequate inventory (in/out) documentation should be maintained when confidential data is removed from secured work environments.
12. No record containing direct personal identifiers (e.g., name, address, SSN or other identifying number) shall be electronically sent to or accessed from a home or telecommuting work site or removed from offices except as required in the conduct of data collection activities, and only in situations where appropriate encryption methods are employed. No confidential information shall reside on a personal or home use computer at any time.

b. Management

1. If confidential data is stored on a mobile device, it is the department's responsibility to ensure that the mobile device supports the Commonwealth approved security and encryption software and that all appropriate information is appropriately encrypted that resides on this device.
2. Physical safeguards (keys, cipher locks, passwords, etc), which are used to secure confidential information, should be changed periodically, and shall be changed every time someone, who formerly had authorized access, either leaves employment, no longer has job requirements which require access, or a key securing such access is lost, stolen or unaccounted for.
3. Enforce appropriate separation of duties involving system access to confidential information. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

4. Restrict access to information system media, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This should also include portable and mobile devices with a storage capability.
5. Protect the security of confidential information at rest, which refers to information stored on a primary or secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.
6. Only a limited number of authorized staff shall have keys or other means of access to cabinets or rooms where equipment containing confidential information is stored.
7. Maintain confidentiality by securely disposing of unnecessary confidential information in an approved manner as it relates to the agency's [Kentucky Department of Library and Archives \(KDLA\) retention schedule](#).
 - a. Remove any confidential and private information that it is no longer needed. This will minimize the liability in case the computer becomes infected or compromised.
 - b. Ensure that confidential or sensitive data is properly cleansed from internal disks or removable media prior to disposal or transfer to others. Seek authoritative advice on disposal of equipment and data. (See [CIO-092 Media Protection Policy](#); [COT-F108 Commonwealth of Kentucky Record of IT Equipment Sanitization Form](#); [NIST SP 800-88 Guidelines for Media Sanitization, Revision 1](#))
8. The authorized head of each agency (agency head) must assure that all employees sign a confidentiality agreement upon hire and annually thereafter. This confirms that the employee has read, fully comprehends and will abide by State policies and procedures regarding privacy and information security.

C. Collection of Confidential Information

1. All confidential information assets must be accounted for and have an assigned owner. Owners, custodians and users of confidential information resources must be identified and their responsibilities defined and documented.

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

2. Only confidential information reasonably necessary to accomplish a legitimate work-related task shall be collected and the time such information is retained shall be limited to that reasonably necessary to achieve such purpose.
3. Before using and/or collecting another agency's confidential information, ensure that all required Confidentiality Agreements are appropriately signed and maintained.
4. When entering or collecting sensitive information from a website, ensure that a secure connection (i.e., https://) has been established.
5. Regularly review holdings of previously collected confidential information to determine whether the information is still relevant and necessary for meeting the agency's business purpose and mission.
6. If the confidential information serves no current business purpose, then the information should no longer be used or collected.
7. Enforce the most restrictive set of rights/privileges, sharing of, or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Access to and sharing of such information should only be granted to authorized individuals on a need to know basis.
8. Prohibit or strictly limit remote access to confidential information. If remote access is permitted, ensure that the communications are encrypted and session activity is logged.
9. Prohibit or strictly limit access to confidential information from portable and mobile devices, such as laptops and smart phones.

D. 6.0 ENFORCEMENT

1. Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal.

IV. REFERENCES

[CIO-072: Identity and Access Management Policy](#)

[CIO-092 Media Protection Policy](#)

[Enterprise Standards and Approved Products 5100: Encryption](#)

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Executive Management
PROCEDURE #1.8	SUBJECT: Storing and Collection of Confidential Information	
EFFECTIVE DATE: 11/29/13; Revised 6/22/16		
CONTACT: Standard Procedures Coordinator		LOCATION: Capital Annex, Room 493 PHONE: 502-564-7236

[KDLA State Government Records Retention Schedules](#)

[NIST SP 800-88 Guidelines for Media Sanitization, Revision 1](#)

[Kentucky's Open Records Act](#) (KRS 61.870 et seq.)

[KRS 61.878\(5\)](#) Sharing of Public Information between Public Agencies

[NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\), April 2010](#)

[The Family Educational Rights and Privacy Act \(FERPA\) of 1974](#) (34 CFR 99.3)

[The Health Insurance Portability and Accountability Act \(HIPAA\) of 1996](#) (Public Law 104-191)

V. FORMS

[COT-F108 Commonwealth of Kentucky Record of IT Equipment Sanitization Form](#)