

| | | |
|--|--|--|
| Finance and Administration Cabinet STANDARD PROCEDURE | | ISSUED BY: Executive Management |
| PROCEDURE #1.6 | SUBJECT: Notification of Personal Information Security Breach | |
| EFFECTIVE DATE: 6/22/16 | | |
| CONTACT: Standard Procedures Coordinator | | LOCATION: Capitol 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

This policy identifies the procedures for Finance and Administration Cabinet (Cabinet) agencies to provide notification of a security breach of personal information.

II. DEFINITIONS

"Agency" means:

- (a) The executive branch of state government of the Commonwealth of Kentucky;
- (b) Every county, city, municipal corporation, urban-county government, charter county government, consolidated local government and unified local government;
- Every organizational unit, department, division, branch, section, unit, office, administrative body, program cabinet, bureau, board, commission, committee, subcommittee, ad hoc committee, council, authority, public agency, instrumentality, interagency body, special purpose governmental entity or public corporation of an entity specified in (a) or (b) or created, established or controlled by an entity specified in (a) or (b).

"Nonaffiliated third party" means any person that:

- Has a contract or agreement with an agency; and
- Receives personal information from the agency pursuant to the contract or agreement.

"Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one or more of the following data elements:

| | | |
|--|--|--|
| Finance and Administration Cabinet STANDARD PROCEDURE | | ISSUED BY: Executive Management |
| PROCEDURE #1.6 | SUBJECT: Notification of Personal Information Security Breach | |
| EFFECTIVE DATE: 6/22/16 | | |
| CONTACT: Standard Procedures Coordinator | | LOCATION: Capitol Annex, Room 493 PHONE: (502) 564-7236 |

- An account number, credit card number or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
- A social security number (SSN);
- A taxpayer identification number that incorporates a SSN;
- A driver's license number, state identification card number or other individual identification number issued by any agency;
- A passport number or other identification number issued by the United States government; or
- Individually identifiable health information (IIHI) as defined in [45 CFR 160.103](#), except for education records covered by the Family Educational Rights and Privacy Act, as amended, [20 USC 1232g](#).

"Security breach" means:

- The unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of unencrypted or unredacted records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality or integrity of personal information and result in the likelihood of harm to one or more individuals; or
- The unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one or more individuals.

"Security breach" does not include the good-faith acquisition of personal information by an employee, agent or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

III. PROCEDURE

A. Notification of a Personal Information Security Breach

1. Cabinet Employees

- a. Employee shall inform next line supervisor.

| | | |
|--|--|--|
| Finance and Administration Cabinet STANDARD PROCEDURE | | ISSUED BY: Executive Management |
| PROCEDURE #1.6 | SUBJECT: Notification of Personal Information Security Breach | |
| EFFECTIVE DATE: 6/22/16 | | |
| CONTACT: Standard Procedures Coordinator | | LOCATION: Capitol Annex, Room 493 PHONE: (502) 564-7236 |

- b. Next line supervisor shall inform management personnel that are responsible for complying with [KRS 61.933 Notification of Personal Information Security Breach](#) and they shall proceed to Section III.A.2.a of this Standard Procedure.

2. Offices and Attached Agencies

- a. Pursuant to [KRS 61.933](#), any agency that collects, maintains or stores personal information that determines or is notified of a security breach relating to personal information collected, maintained or stored by the agency or by a nonaffiliated third party on behalf of the agency shall as soon as possible, but within 72 hours of determination or notification of the security breach:
- b. Notify the commissioner of the Kentucky State Police, the Auditor of Public Accounts (APA) and the Attorney General. In addition, an agency shall notify the secretary of the Cabinet or his/her designee if an agency is an organizational unit of the executive branch of state government or notify the commissioner of the Department for Local Government if the agency is a unit of government listed in [KRS 61.931\(1\)\(b\) or \(c\)](#) that is not an organizational unit of the executive branch of state government.
- c. Notification shall be in writing on the Commonwealth Office of Technology's (COT) [Determined Breach Notification Form](#) (FAC-001); and
- d. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices referenced in [KRS 61.932\(1\)\(b\)](#) to determine whether the security breach has resulted in or is likely to result in the misuse of the personal information.

3. Upon conclusion of the agency's investigation:

- a. If the agency determined that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:
 - 1. Within 48 hours of completion of the investigation, notify in writing all officers listed in [KRS 61.933\(1\)\(a\)\(1\)](#), and the commissioner of the Kentucky Department for Libraries and Archives (KDLA), unless the provisions of [KRS 61.933\(3\)](#) apply;
 - 2. Within 35 days of providing the notifications required by [KRS](#)

| | | |
|--|--|--|
| Finance and Administration Cabinet STANDARD PROCEDURE | | ISSUED BY: Executive Management |
| PROCEDURE #1.6 | SUBJECT: Notification of Personal Information Security Breach | |
| EFFECTIVE DATE: 6/22/16 | | |
| CONTACT: Standard Procedures Coordinator | | LOCATION: Capitol Annex, Room 493 PHONE: (502) 564-7236 |

[61.933\(1\)\(b\)\(1\)\(a\)](#), notify all individuals impacted by the security breach as provided in [KRS 61.933\(2\)](#), unless the provisions of [KRS 61.933\(3\)](#) apply; and

3. If the number of individuals to be notified exceeds 1,000, the agency shall notify, at least seven days prior to providing notice to individuals under [KRS 61.933\(1\)\(b\)\(1\)\(b\)](#), the COT if the agency is an organizational unit of the executive branch of state government or the Department for Local Government if the agency is a unit of government listed under [KRS 61.931\(1\)\(b\) or \(c\)](#) that is not an organizational unit of the executive branch of state government; and notify all consumer credit reporting agencies included on the list maintained by the Office of the Attorney General that compile and maintain files on consumers on a nationwide basis, as defined in [15 USC 1681a\(p\)](#), of the timing, distribution and content of the notice; or
 - b. If the agency determines that the misuse of personal information has not occurred and is not likely to occur, the agency is not required to give notice, but shall maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by [KRS 171.420](#). The agency shall notify the appropriate entities listed in [KRS 61.933\(1\)\(a\)\(1\)](#) that the misuse of personal information has not occurred.
3. Pursuant to [KRS 61.933\(6\)](#), the Office of the Attorney General may bring an action in the Franklin Circuit Court against an agency or a nonaffiliated third party that is not an agency, or both, for injunctive relief, and for other legal remedies against a nonaffiliated third party that is not an agency to enforce the provisions of KRS 61.931 to KRS 61.934. Nothing in KRS 61.931 to KRS 61.934 shall create a private right of action.

B. The Kentucky Whistleblower Act (KRS 61.101 et seq.)

1. The Cabinet is committed to operating in compliance with all applicable laws, rules and regulations, and it prohibits unlawful retaliatory practices against its employees by any of its board members, officers, employees or agents. Employees may report any actual or suspected violations of law or policy, or any facts or information relative to actual or suspected mismanagement, waste, fraud, abuse of authority or substantial and specific danger to public health or safety to any public body with apparent authority to remedy or report such actions. This policy applies to any matter which is related to the cabinet's business and does not relate to private acts of an individual not connected to the business of the Cabinet.

| | | |
|--|--|--|
| Finance and Administration Cabinet STANDARD PROCEDURE | | ISSUED BY: Executive Management |
| PROCEDURE #1.6 | SUBJECT: Notification of Personal Information Security Breach | |
| EFFECTIVE DATE: 6/22/16 | | |
| CONTACT: Standard Procedures Coordinator | | LOCATION: Capitol Annex, Room 493 PHONE: (502) 564-7236 |

2. Pursuant to [KRS 61.102](#), the Cabinet will not subject any employee, as defined in [KRS 61.101](#), to reprisal, either directly or indirectly, or threatening to use, for having made a good faith report of suspected wrongdoing of the type set-forth above, either internally to the Cabinet, or externally to any public body with apparent authority to remedy or report such wrongdoing, nor will the Cabinet take any such retaliatory action against any person who supports, aids or substantiates such an employee in having done so.

IV. REFERENCES

[KRS 61.931](#) Definitions for KRS 61.931 to KRS 61.934

[45 CFR 160.103](#) Definitions

[20 USC 1232g](#) Family educational and privacy rights

[KRS 61.933](#) Notification of personal information security breach

[KRS 61.932](#) Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties

[15 USC 1681a\(p\)](#) Definitions; Rules of construction; Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis

[KRS 171.420](#) State Archives and Records Commission

[KRS 61.102](#) Reprisal against public employee for disclosure of violations of law prohibited

[Guide to the Executive Branch Code of Ethics](#)

V. FORMS

[Determined Breach Notification Form](#) (FAC-001) Form to report a security breach