Information Security Policy and Procedures Checklist

With the passage of HB5 in the 2014 session of the KY Legislature, the Kentucky Department for Local Government (DLG) was charged with developing policies to establish security and breach investigation procedures and practices for local government agencies [KRS 61.932(1)(b)], and responded with *Protection of Personal Information: Security and Incident Investigation Procedures & Practices for Local Government Units*.

Each Local Government Unit (LGU) which includes Special Purpose Government Entities (SPGEs) is responsible to ensure the security of all personal data in any format or medium that is collected to conduct business and to also investigate and report any breaches of security to the proper authorities and to affected individuals.

This document seeks to provide an overview of the guidance from the DLG best practices document. Any questions regarding the implementation of the DLG's policy should be directed to the DLG's Office of Legal Services for further explanation or clarification.

Policy

- ☐ The library has adopted the *Protection of Personal Information* policy created by the DLG or has adopted a more stringent policy. KRS 61.932(1)(b)
  - ☐ The DLG policy is reviewed at least annually for changes.
  - ☐ The library's policy is reviewed annually to ensure compliance with any necessary changes.
- ☐ All library personnel and contractors or others with access to personal information in the library's possession will be informed of this policy and required to follow proper security procedures.
- ☐ As of January 1, 2015, any new and/or amended agreements or contracts with vendors will require that they adopt security and breach investigation policies at least as stringent as those required by KY Statute. KRS 61.932(2)

Point of Contact

- ☐ In compliance with DLG guidance, the library has appointed a Point of Contact Officer (POC) who:
  - ☐ maintains the information security policy;
  - ☐ is the contact for inquiries from other agencies regarding the information security policy or security breach incidents;
  - ☐ ensures that library staff understand the information security policy;
  - ☐ ensures compliance with the information security policy; and,
  - ☐ responds to incidents where there is a breach of security of personal information.

Security of Data

- ☐ The library stores all personal information securely – both non-digital and digital – to prevent unauthorized access.
  - ☐ All paper records containing personal information is stored in locked rooms, cabinets, or drawers with access limited to authorized personnel only.
  - ☐ All electronic records storing personal information is protected by software to prevent unauthorized access.
  - ☐ All e-mail or other electronic transmission of personal information is encrypted to prevent unauthorized access.

Physical Security

- ☐ The library has established and maintains physical security procedures to protect its records which address natural disasters, fire, electrical outages, or other physical threats to information resources.
- ☐ The library's physical security procedures address security measure required to prevent unauthorized access to, physical tampering, damage, or theft of information resources.
  - ☐ This may include establishing parameters of physical access and ID badge requirements for access to these areas.
  - ☐ Information technology equipment will be marked as the library's property.

Access Control

- ☐ Only authorized individuals are permitted access to media containing personal information.
- ☐ User authentication provides audit access information and complies with regulatory requirements.

Software

- ☐ The library uses security software to protect personal information that provides user identification, authentication, data access controls, integrity, and audit controls.
  - ☐ Security software is tested to confirm functionality and contractual provisions also ensure that the supplier's software, by design or configuration, will not introduce any security exposures.
  - ☐ The level of protection afforded by security software is commensurate with the sensitivity of the data.
  - ☐ These issues are addressed before any personal data is stored on a device.
- ☐ The library's systems, networks and application software used to process personal information adhere to the highest level of protection reasonably practical.
  - ☐ The library uses Intrusion Detection and Prevention software, such as McAfee Network Security Manager, or others comparable to those approved by the

Commonwealth Office of Technology (COT) as outlined in the Enterprise Architecture and Kentucky Information Technology Standards (KITS).

Encryption

- ☐ The library stores Information on digital media that is encrypted in accordance with contemporary standards.

Portable Computing Devices

- ☐ The library prohibits the unnecessary placement (download or input) of personal information on portable computing devices, such as: laptops, tablet computers, digital cameras, cell phones, and other electronic devices on which personal media could be stored.
  - ☐ When personal information must be placed on portable computing devices to conduct library business, the library will ensure that the employee is aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information.
    - ☐ If personal information is placed on a portable computing device, every effort will be taken, including physical controls, to protect the information from unauthorized access.
    - ☐ The library will make every effort to minimize the amount of information required. If possible, information will be abbreviated to limit exposure (e.g., last 4 digits of the social security number).
    - ☐ The library ensures that the portable computing device supports appropriate data encryption software and that all information on the device is encrypted.
  - ☐ Each person using a portable computing device will sign a library-approved form indicating acceptance of the information and acknowledging his/her understanding of the responsibility to protect the information.
    - ☐ This form is reviewed and renewed annually.
- ☐ In the event the portable computing device is lost or stolen, the library will be able to recreate the personal information with 100 percent accuracy and must be able to provide notification to all affected persons/entities.

Destruction of Records Containing Personal Information

- ☐ The library follows the Local Government Records Retention Schedule, Administration, Series L6709: Personal Information Security Breach Investigation/Notification File.
  - ☐ The library will destroy records containing personal or confidential information completely to ensure that the information cannot be recognized or reconstructed
  - ☐ Any personal or confidential data contained on the computer media will be obliterated and/or made indecipherable before disposing of the tape, diskette, CD-ROM, zip disk, or other type of medium.
- ☐ The library provides appropriate methods and equipment to routinely destroy personal or confidential information using one of the following safeguards listed below. The methods set forth below by the Department for Local Government are listed in priority order with the most highly recommended safeguard listed first.

1. Conduct due diligence and hire a document destruction contractor to dispose of material either offsite or onsite.
2. Require that the disposal company be certified by a recognized trade association.
3. Require and validate that the disposal company disk sanitizing software and/or equipment is approved by the United States Department of Defense.
4. Review and evaluate the disposal company's information security policies and procedures.
5. Review an independent audit of a disposal company's operations and/or its compliance with nationally recognized standards.
6. Secure and utilize shredding equipment that performs cross-cut or confetti patterns.
7. Secure and utilize a disk sanitizing (i.e., erasing) software program approved by the United States Department of Defense.
8. Secure and utilize disk erasing equipment (e.g. degausser) approved by the Department of Defense or the National Security Agency.
9. Modify the information to make it unreadable, unusable or indecipherable through any means.

For information on Investigating and Reporting Security Breaches, see the *Security Breach Reporting Checklist.*