Security Breach Reporting Checklist

The Library is required under KRS 61.933 to disclose a security breach in which personal information in any format is disclosed to, or obtained by, an unauthorized person. State authorities and affected individuals (customers or staff) will be notified as outlined below.

Notifying State Officials

When the Library identifies that a security breach has occurred in which personal information has been disclosed to, or obtained by, an unauthorized person, it shall:

- Within 72 hours, notify the following in writing using FAC-001, Determined Breach Notification Form:
  - ☐ The commissioner of the Kentucky State Police,
  - ☐ The Auditor of Public Accounts,
  - ☐ The Attorney General, and
  - ☐ The commissioner of the Department for Local Government.

- Within 72 hours, begin conducting a prompt investigation to determine whether or not the security breach has resulted in, or is likely to result in, the misuse of the personal information. The Library shall document the following:
  - ☐ Preliminary Reporting and description of the incident;
  - ☐ Response, including evidence gathered;
  - ☐ Final Assessment and corrective action taken; and
  - ☐ Final Reporting

If the Library determines that **the misuse of information has occurred** or is likely to occur:

- Within 48 hours of completion of the investigation, notify using FAC-001, Determined Breach Notification Form:
  - ☐ The commissioner of the Kentucky State Police,
  - ☐ The Auditor of Public Accounts,
  - ☐ The Attorney General,
  - ☐ The commissioner of the Department for Local Government, and
  - ☐ The commissioner of the Kentucky Department for Libraries and Archives.
- Affected Individuals as outlined below.

If the Library determines that **the misuse of personal information has not occurred** and is not likely to occur, the Library is not required to give notice to affected individuals, but shall:

☐ Notify, using FAC-001, Determined Breach Notification Form:
  - ☐ The commissioner of the Kentucky State Police,
  - ☐ The Auditor of Public Accounts,
  - ☐ The Attorney General, and
  - ☐ The commissioner of the Department for Local Government that the misuse of personal information has not occurred.

☐ Maintain records that reflect the basis for its decision for a retention period provided in the appropriate retention schedule. Refer to the Local Government General Records Schedule (Series L6709 – Personal Information Security Breach Investigation/Notification File) and the General Schedule for Electronic Records and Related Records for more information.

Notifying Affected Individuals

Within thirty-five days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal information will be sent by the Library describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information. Notification may be delayed in two circumstances, and the Library must complete FAC-002, Delay Notification Record if either circumstance occurs:

- If law enforcement makes a written request due to a criminal investigation (KRS 61.933 (3)(a)) or
- The Library determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within 35 days AND the Office of the Attorney General has approved the delay in writing (KRS 61.933 (3)(b))

Unless one of the two circumstances allowing delayed notification occurs, the Library will provide notification as follows within 35 days of detection of the incident:

- ☐ A notice will be posted in a conspicuous place on the Library's website.
- ☐ Notification will be provided to regional and local media, including broadcast media (TV, radio), if the breach is localized and also to statewide media if the breach is widespread.
- ☐ Personal communication to the individuals whose information has been breached using one of the following methods which the Library believes to be the most likely to result in actual notification:
    - ☐ In writing, sent to the most recent address in the Library's records
    - ☐ By email, to the most recent email address unless the person has requested in writing that they do not want email notification
    - ☐ By telephone, to the most recent phone number in the Library's records.

The notice will include:

- ☐ To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;
- ☐ Contact information for the Library, including the address, telephone number, and toll-free number if a toll-free number is maintained;
- ☐ A description of the general acts of the Library, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and
- ☐ The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
    - ☐ The major consumer credit reporting agencies;
    - ☐ The Federal Trade Commission; and
    - ☐ The Office of the Kentucky Attorney General.

If more than 1,000 individuals will be notified, at least 7 days prior to providing the notices the Library will notify:

- ☐ The Department for Local Government.
- ☐ 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 U.S.C. sec. 1681a(p), of the timing, distribution, and content of the notice.

Disclosure Communications

Within the parameters of the law, minimal disclosure regarding incidents is preferred to prevent unauthorized persons from acquiring sensitive information regarding the incident, security protocols and similar matters, in an effort to avoid additional disruption and financial loss.

Commonwealth Office of Technology

The Commonwealth Office of Technology (COT) is responsible for creating and maintaining the forms FAC-001, Determined Breach Notification Form and FAC-002, Delay Notification Record. For questions about completing those forms, contact the COT Office of the Chief Information Security Officer (CISO) at COTSecurityOperations@ky.gov or (502) 564-1532.

[Reviewed 02/16/2023]