Information Security Policy

KDLA provides this example policy to assist a library in developing and adopting their own policy. The example policy should be modified to meet the needs of your library and community and should be reviewed by the library's attorney prior to adoption.

In accordance with KRS 61.931-934, _____ Public Library will take reasonable precautions to ensure that any personal information that is kept by the library for any purpose is safeguarded from unauthorized access.

_____ Public Library will comply with best practices established by the Department for Local Government (as required in KRS 61.932). See *Security and Incident Investigation Procedures and Practices for Local Governmental Units* for these best practices.

Per the Department of Local Government's guidance, a "Point of Contact" is designated by _____ Public Library to

1) Maintain the library's adopted Information Security Policy and be familiar with its requirements;
2) Ensure the library's employees and others with access to personal information are aware of and understand the Information Security Policy;
3) Serve as contact for inquiries from other agencies regarding its Information Security Policy and any incidents;
4) Be responsible for ensuring compliance with the Information Security Policy; and 5) Be responsible for responding to any incidents.

The (Designated Individual) is _____ Public Library's Point of Contact for the purpose of adherence to Department for Local Government guidance.

Patron information

_____ Public Library acts to limit the amount of personally identifiable information that it retains. Some information, however, is necessarily and understandably retained for the transaction of day to-day business.

Most information related to patrons is kept for the purposes of circulating materials and ensuring that responsibility is attributed to the correct person when an item is borrowed. This information is not publicly available and, beyond interactions between the library and the patron, will be shared only with third-party vendors with whom the library has contracted services necessary for conducting business and law enforcement personnel upon valid, legal request. Information related to delinquent patrons may be shared with a third party vendor for the purposes of collection. The library will not share personally identifiable patron information for any other purpose.

When a patron record has been inactive for (specify years) _____ and carries no outstanding debt (financial or in borrowed materials), the record is deleted from the library's computer system and is not archived.

Personal information about patrons is generally only retained in electronic format with appropriate back-up devices in place for recovery in the event of a database failure. All back-up devices are kept secured at all times in areas that are not accessible to the general public and with limited accessibility by staff.

Staff information

_____ Public Library retains information about its staff that is directly related to the work environment. Social security numbers, health information, and performance records are retained only as a part of standard human resources processes (such as payroll, retirement, or health insurance). This information is subject to records retention policies of the Commonwealth of Kentucky and _____ Public Library. Records will be retained and destroyed according to the records retention schedule.

Personal information about staff members is, in some cases, subject to the Open Records Act and will be shared with anyone properly requesting that information as specified by Kentucky Revised Statute. Information protected from disclosure under the Open Records Act will not be shared with any outside agency for any purpose other than for the reason it was collected (i.e. to a payroll vendor for tax purposes).

Personal information about staff will be kept secured at all times in areas that are not accessible to the general public and with limited accessibility by staff.

Security Measures

The library does not share any information with any outside agency for any reason other than the purposes for which it was collected. Third party vendors with whom the library does business are required by KRS 61.932 to provide their own security measures to protect any personal information. Where possible, the library has informed each entity in writing that appropriate security and breach notification is required.

The library provides an internal, closed network for the collection and use of most patron data. The network is not accessible to the general public and access to it is limited to third party vendors with whom the library has contracted services.

Where the library's systems do have interaction with any outside vendor or patron (i.e. through the internet-based catalog), transactions will take place using secure transmission protocols. Such interactions will be limited to the purpose of the transaction only and will not allow access to any more information than is required for

the purpose of the transaction (i.e. a patron reviewing a list of items that are currently checked out to him/her).

Personal information stored on computers or back-up devices is not accessible to the general public and is protected by a computer firewall and anti-virus systems.

Security Breaches and Notifications

If _____ Public Library becomes aware of a breach that would allow outside access to its network or access to devices used to store personal information, action will immediately be taken to remove the device from the network or to close the network to all external traffic.

_____ Public Library will notify vendors of their responsibilities to inform the library of any breach in their own systems which would expose or compromise the security of personal information provided by the library. Notification of such must conform to the requirements of KRS 61.932 and will include any reports of investigations that are conducted into the breach. Contracts that are made or amended with the library after January 1, 2015 must contain provisions to account for the requirements under KRS 61.932.

In the event _____ Public Library's own computer network or data storage systems are breached, the library will immediately take action to secure the network or system, to prohibit any off-site access, and to determine the extent of the data that was obtained by the unauthorized party.

Where appropriate, the library will notify any/all affected parties within the guidelines of KRS 61.933 or as directed in guidance from the Department for Local Government. Investigations which follow such a breach will be reported as required by the same statute.

[Reviewed 5/13/2015]