KDLA Trustee Tip of the Month – April 2015
Information Security Requirements for Public Libraries

As Special Purpose Governmental Entities increasingly collect sensitive personal information about clients and employees in electronic and paper formats, the risk of a data breach grows. 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 and practices to guide local government agencies in developing security and breach protocols for prevention of and response to potential data breaches (KRS 61.932[1][b]).

To assist public libraries in meeting their responsibilities under HB5 and its corresponding statutes, KDLA has developed a series of documents that satisfy public libraries' obligations to protect sensitive data and to report data breaches. These documents include:

Information Security Policy

In accordance with KRS 61.931-934, public libraries must take every reasonable precaution to safeguard personal information about patrons and employees in any format from unauthorized access. Statute also requires public libraries to comply with best practices established by the DLG in *Security and Incident Investigation Procedures and Practices for Local Governmental Units*. The Information Security Policy developed by KDLA acknowledges libraries' responsibility to comply with the DLG best practices, while also establishing baseline policy that guides libraries in the safekeeping of all patron and employee data. **Adopting this policy will establish libraries' compliance with DLG best practices as required by statute.**

Information Security Policy and Procedures Checklist

The Information Security Policy and Procedures Checklist acts as guidance to following the Information Security Policy, and includes the procedures necessary to implementing the policy as part of library operations. Trustees and library employees may find this checklist particularly helpful in understanding some of the requirements of KRS 61.931-934.

Security Breach Reporting Checklist

Public libraries are required under KRS 61.933 to disclose security breaches in which personal information in any format is disclosed to, or obtained by, an unauthorized person. This disclosure requirement includes reporting any security breaches to specific authorities and affected individuals. The Security Breach Reporting Checklist presents the required reporting obligations in an easy-to-follow format. **Following the Security Breach Reporting Checklist in the event of a data breach can help ensure compliance with KRS 61.933.**

Libraries have historically been dedicated to preserving the confidentiality of patron records. Adopting and enforcing an information security policy mandates that dedication to confidentiality, both for patrons and employees while helping protect libraries from costly data breaches.

This is not legal advice. If you feel you need legal advice you should consult an attorney.