Kentucky League of Cities, Inc.
Personally Identifiable Information Breach Notification Policy

In an effort to protect individuals from the growing threat of identity theft caused by data breaches, if personally identifiable information (PII) is breached Kentucky League of Cities, Inc. (KLC) adheres to the notification requirements defined in House Bill 232 passed by 2014 General Assembly relating to security breach notifications.

PII is defined in the statute as:
'Personally identifiable information' means an individual´s first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: (1) Social security number; (2) Driver´s license number; (3) Account number, credit or debit card number, in combination with any security code, access code, or password permit access to an individual's financial account.

Breach of the security of the system is defined in the statute as:
'Breach of the security of the system' means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure.

KLC, upon determining that PII has been breached, adheres to HB 232's notification requirements:
KLC may utilize two primary notice methods and/or three substitute notice methods as provided in the statute. The primary notice methods are written notice or electronic notice. However, electronic notice only may be given if the consumer consented in advance, as outlined in 15 U.S.C.A. § 7001, to receive electronic notices in lieu of paper.

Substitute notice methods may be used by KLC if: (i) the cost of giving notice through one of the primary methods exceeds $250,000; (ii) there are more than 500,000 individuals affected; or (iii) sufficient contact information is not available to provide primary notice. E-mail, conspicuous posting of the notice on the entity's webpage, and/or notification of state-wide media, consistent with HB 232's notice timing requirements, are acceptable substitute notice methods.

Following FTC regulations, the notice from KLC will be easy to understand and will include:

1) a brief description of what happened, including the date of the breach (if known) and the date the breach was discovered;
2) the kind of information involved in the breach (i.e. Social Security numbers, financial account data, dates of birth, medication information, etc.);
3) suggested steps affected individuals can take to protect themselves. KLC's advice will be relevant to the kind of information that was compromised; and
4) KLC's toll-free telephone number, email address, website, or mailing address.

If more than 1,000 individuals at one time require notification under this policy, KLC will notify all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis as required in HB 232.