Commonwealth of Kentucky
FINANCE AND ADMINISTRATION CABINET
Office of the Controller
Office of Procurement Services
Room 096 Capitol Annex
Frankfort, Kentucky 40601
(502) 564-4510
(502) 564-1434 Facsimile

STEVEN L. BESHEAR
Governor

Lori H. Flanery
Secretary

Ed Ross
Executive Director

Don Speer
Executive Director

TO: **All Agency Purchasing Contacts**

FROM: Donald R. Speer, Executive Director
Office of Procurement Services

DATE: January 9, 2015

SUBJECT: Protection of Personal Information Security and Breach Investigation Procedures and Practices Act

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, et seq.) went into effect. This Act concerns the protection of personal information and applies to every state agency and university.

For all solicitations issued by a state agency where it is anticipated that the state agency, in the resulting contract, will disclose "personal information" (defined below), and for all contracts executed or amended on or after January 1, 2015, with a "non-affiliated third party" (defined below) to whom the state agency discloses "personal information" (defined below), the following provisions shall be included:

Vendors that receive Personal Information as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), shall secure and protect the Personal Information by, without limitation, complying with all requirements applicable to non-affiliated third parties set forth in the Act.

"Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

a) An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
b) A Social Security number;
c) A taxpayer identification number that incorporates a Social Security number;

d) A driver's license number, state identification card number or other individual identification number issued by an agency;
e) A passport number or other identification number issued by the United States government; or
f) Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

As provided in KRS 61.931(5), a "non-affiliated third party" means "any person or entity that has a contract or agreement with the Commonwealth and receives (accesses, collects or maintains) personal information from the Commonwealth pursuant to the contract or agreement."

The vendor hereby agrees to cooperate with the Commonwealth in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

The vendor shall notify as soon as possible, but not to exceed seventy-two (72) hours, the contracting agency, the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Commonwealth Office of Technology of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)2 applies and the vendor abides by the requirements set forth in that exception. If the agency is a unit of government listed in KRS 61.931(1)(b), the vendor shall notify the Commissioner of the Department of Local Government in the same manner as above. If the agency is a public school district listed in KRS 61.931(1)(d), the vendor shall notify the Commissioner of the Department of Education in the same manner as above. If the agency is an educational entity listed under KRS 61.931(1)(e), the vendor shall notify the Council on Postsecondary Education in the same manner as above. Notification shall be in writing on a form developed by the Commonwealth Office of Technology http://finance.ky.gov/services/forms/Pages/default.aspx **.**

The vendor hereby agrees that the Commonwealth may withhold payment(s) owed to the vendor for any violation of the Identity Theft Prevention Reporting Requirements.

The vendor hereby agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

Upon conclusion of an investigation of a security breach of Personal Information as required by KRS 61.933, the vendor hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.

In accordance with KRS 61.932(2)(a) the vendor shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the

information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth Office of Technology:

http://technology.ky.gov/ciso/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx

State agencies may access these provisions in eMARS. You can access these provisions from the Terms and Conditions section of your document by inserting a line in the Terms and Conditions section, clicking the T and C pick list icon and selecting "Personal Information Security and Breach". Assemble your document as normal after including other necessary information. Detailed instructions will be available on the Office of Procurement Services website: http://finance.ky.gov/offices/controller/Pages/ops.aspx

As stated previously, the above language should **only** be included in solicitations and contracts that include or will include information that meets the definition of "personal information" as defined in KRS 61.931(6). If you have any questions concerning whether one or more of your agency's contracts meet the definition of "personal information" please contact the Office of the Chief Information Security Office, 502 564-6361. katrina.lemay@ky.gov In addition, you should consult with your agency General Counsel regarding any provisions of the Act.