61.932 Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties.

(1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.

(b) Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology. Reasonable security and breach investigation procedures and practices established and implemented by units of government listed under KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government shall be in accordance with policies established by the Department for Local Government. The Department for Local Government shall consult with public entities as defined in KRS 65.310 in the development of policies establishing reasonable security and breach investigation procedures and practices for units of local government pursuant to this subsection. Reasonable security and breach investigation procedures and practices established and implemented by public school districts listed under KRS 61.931(1)(d) shall be in accordance with administrative regulations promulgated by the Kentucky Board of Education. Reasonable security and breach investigation procedures and practices established and implemented by educational entities listed under KRS 61.931(1)(e) shall be in accordance with policies established by the Council on Postsecondary Education. The Commonwealth Office of Technology shall, upon request of an agency, make available technical assistance for the establishment and implementation of reasonable security and breach investigation procedures and practices.

(c) 1. If an agency is subject to any additional requirements under the Kentucky Revised Statutes or under federal law, protocols, or agreements relating to the protection and privacy of personal information, the agency shall comply with these additional requirements, in addition to the requirements of KRS 61.931 to 61.934.

2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one (1) or more data elements of personal information that is the same as one (1) or more of the data elements of personal information listed in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the requirements of KRS 61.931 to 61.934 by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph

shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in KRS 61.931(6)(a) to (f).

(2) (a) For agreements executed or amended on or after January 1, 2015, any agency that contracts with a nonaffiliated third party and that discloses personal information to the nonaffiliated third party shall require as part of that agreement that the nonaffiliated third party 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 referenced in subsection (1)(b) of this section, and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

(b) 1. A nonaffiliated third party that is provided access to personal information by an agency, or that collects and maintains personal information on behalf of an agency shall notify the agency in the most expedient time possible and without unreasonable delay but within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the nonaffiliated third party has with regard to the security breach at the time of notification. Agreements referenced in paragraph (a) of this subsection shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.

2. The notice required by subparagraph 1. of this paragraph may be delayed if a law enforcement agency notifies the nonaffiliated third party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subparagraph, notification shall be given as soon as reasonably feasible by the nonaffiliated third party to the agency with which the nonaffiliated third party is contracting. The agency shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form.

Effective: January 1, 2015

History: Created 2014 Ky. Acts ch. 74, sec. 2, effective January 1, 2015.

Legislative Research Commission Note (1/1/2015). 2014 Ky. Acts ch. 74, sec. 10 provided that "the provisions of this Act shall not impact the provisions of KRS 61.870 to 61.884." That proviso applies to this statute as created in Section 2 of that Act.