4121-4-05 Restricting and logging access to confidential personal information in computerized personal information systems.

Effective: October 1, 2010

For personal information systems that are computer systems and contain confidential personal information, the commission shall do the following:

(A) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(B) Acquisition of a new computer system. When the commission acquires a new computer system that stores, manages or contains confidential personal information, the commission shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.

(C) Upgrading existing computer systems. When the commission modifies an existing computer system that stores, manages or contains confidential personal information, the commission shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.

(D) Logging requirements regarding confidential personal information in existing computer systems.

(1) The commission shall require employees of the commission who access confidential personal information within computer systems to maintain a log that records that access.

(2) Access to confidential information is not required to be entered into the log under the following circumstances:

(a) The employee of the commission is accessing confidential personal information for official commission purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(b) The employee of the commission is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(c) The employee of the commission comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(d) The employee of the commission accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(i) The individual requests confidential personal information about himself/herself.

(ii) The individual, or his or her authorized representative, makes a request that the employee of the commission take some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(3) For purposes of this paragraph, the commission may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management. The commission shall issue a policy that specifies the following:

(1) Who shall maintain the log;

(2) What information shall be captured in the log;

(3) How the log is to be stored; and

(4) How long information kept in the log is to be retained.

Nothing in this rule limits the commission from requiring logging in any circumstance that it deems necessary.