



## Ohio Administrative Code

### Rule 1501-8-05 Restricting and logging access to confidential personal information in computerized personal information systems.

Effective: September 17, 2010

---

For personal information systems that are computer systems and contain confidential personal information, the department 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 department acquires a new computer system that stores, manages or contains confidential personal information, the department shall include a mechanism for recording specific access by employees of the department to confidential personal information in the system.
- (C) Upgrading existing computer systems. When the department modifies an existing computer system that stores, manages or contains confidential personal information, the department 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 department to confidential personal information in the system.
- (D) Logging requirements regarding confidential personal information in existing computer systems.
  - (1) The department shall require employees of the department 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 department is accessing confidential personal information for official department 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 department 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 department 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 department 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 that individual.
  - (ii) The individual makes a request that the department takes 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 department may choose the form or forms of logging, whether in electronic or paper formats.
- (E) Log management. The department 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.
- (F) Nothing in this rule limits the department from requiring logging in any circumstance that it deems necessary.