

IPP.3922. Code of Responsibility

IPPMTL 0249

July 19, 2011 - Revised

May 9, 2003 - Original

CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.

I. PURPOSE:

- A. To inform all ODJFS system users (ODJFS state employees, temporary service personnel, contractor personnel, county users, business partners, and external agencies) of their responsibility for maintaining the security of all personal information (hard-copy and electronic) to which they have access in the course of performing their work.
- B. To provide the revised form JFS 07078 - OHIO DEPARTMENT OF JOB AND FAMILY SERVICES CODE OF RESPONSIBILITY (see Appendix B) which describes the specific information and confidentiality requirements to which all ODJFS system users (ODJFS employees, temporary service personnel, contractor personnel, county users, business partners, and external agencies) must subscribe in order to gain access to ODJFS and specific State of Ohio computer systems.

II. REFERENCE/AUTHORITY:

A. REFERENCES

Note: References to the Ohio Revised Code (ORC) can be accessed at the following website:

<http://codes.ohio.gov/> .

1. Information Technology Policy ITP E.8, Use of Internet, E-mail and Other IT Resources, published by The Ohio Department of Administrative Services, dated March 19, 2008.
2. Internal Revenue Code, Section 7213 (a).
3. Ohio Revised Code (ORC) [5101.02](#) , [5101.27](#) through [5101.31](#) , [5101.99](#) , [3107.17](#) , [3107.42](#) , [3107.99](#) , [3121.894](#) , [3121.899](#) , [3121.99](#) , [3125.08](#) , [3125.50](#) , [3125.99](#) , [4141.21](#) , [4141.22](#) and [4141.99](#)
4. Code of Federal Regulations: 45 CFR 160 and 164 (HIPAA-45 CFR164.501); 42 CFR 431.300 through 431.307; 5 USC 552a; 7 CFR 272.1(c)
5. Ohio Administrative Code (OAC) rules [4141-43-01](#) through [4141-43-03](#)
6. [IPP 3001](#) ODJFS Information Security
7. [IPP10002](#) Computer Usage and Information System Usage
8. [IPP 3925](#) ODJFS Data Access Policy
9. [IPP 10004](#) Incident Reporting
10. [IPP 8106](#) Research and Research Data Approval

B. AUTHORITY

Exhibit 2

Page 2 of 4

This policy is established by order of the director, ODJFS, hereinafter referred to as director.

Per ORC 5101.02, all duties conferred on the various work units of the department by law or by order of the director shall be performed under such rules as the director prescribes and shall be under the director's control.

III. **SUPERSEDES:**

ODJFS-IPP 3922 ODJFS Code of Responsibility dated May 5, 2010.

IV. **SCOPE:**

This procedure applies to all ODJFS system users as noted in Section I (A) of this policy.

NOTE: Requirements for county users, business partners, and external agencies also specified under Administrative Rule.

NOTE: County users, business partners, and external agencies must follow any applicable Ohio Administrative Code rules regarding data access. (Ohio Revised Code (ORC) - 1347.15)

V. **DEFINITIONS:**

A. County Local Security Coordinators

The County partner representative, as defined in the OIS Service Level Agreement, is the point of contact with the ODJFS OIS Access Control for all security issues.

B. Office Information Services (OIS)

OIS is responsible for developing, maintaining, and supporting ODJFS applications. Access Control is a unit contained within the Bureau of Production and Operations, Office of Information Systems, which is responsible for provisioning and de-provisioning functions as they relate to application and data access.

C. State Point of Contact

The state manager representative of an external entity or specific areas of ODJFS. The state manager is held accountable for the external users access to the internal ODJFS network and internal ODJFS applications. The state manager is responsible for notifying OIS Access Control of personnel changes and contract amendments/terminations /extensions with the external entity.

D. External Entity

An external business partner or external sister agency requiring access to the ODJFS internal network and/or internal applications.

VI. **PROCEDURES:**

A. All ODJFS system users (as noted in I.A.) must complete the JFS 07078 - ODJFS Code of Responsibility Any access to information about recipients of ODJFS benefits or services, or about ODJFS employees, that is collected and maintained on ODJFS or state computer systems is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's **official** job duties and work assignments **for, and on behalf of**, ODJFS and/or a federal oversight agency.

It serves several purposes:

1. The form provides the statement of understanding concerning the confidentiality

and security of data and the acknowledgment of that statement by the individual.

2. It is used to establish or change access to specific ODJFS or State of Ohio systems for ODJFS system users (as noted in I.A.).
- B. Any access to information about recipients of ODJFS benefits or services, or about ODJFS employees, that is collected and maintained on ODJFS or state computer systems is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's **official** job duties and work assignments **for, and on behalf of**, ODJFS and/or a federal oversight agency.
 - C. This form is completed for state employees when a new hire initially reports to the ODJFS Office of Employee and Business Services for in-processing. Upon completion of the form, the Human Resources (HR) representative will sign, then fax or email the JFS 07078 along with a Confirmation Letter to the OIS Access Control Unit. The Access Control Unit will grant a Novell Network, GroupWise and Confidential Personal Information (CPI) LOG Accounts and notify both the HR Representative and the employee's supervisor of the Novell Network ID.
 - D. Change requests, including modifications to existing access, must be submitted using the JFS 07078 and be completed by the unit supervisor and sent to Access Control.
 - E. If this system access request is originating from a county office, business partner, external agency, or specific areas of ODJFS; then it must be first directed to their Local Security Coordinator (Security Point of Contact) or State Point of Contact for signature approval. Then the JFS 07078 form along with a cover memo from the Local Security Coordinator or State Point of Contact detailing the system access requested shall be mailed, faxed, or emailed, to the Access Control Unit, Production and Operations, Office of Information Services at the address indicated on the information security web page: <http://innerweb/omis/InfoSecurity/InfoSecindex.shtml>.
 - F. The responsibility for forwarding completed JFS 07078 forms and associated cover memos belongs to the State employee's supervisor, the county equivalent Local Security Coordinator (LSC), or designated State Point of Contact as listed above.
 - G. If a specific copy of a completed and approved JFS 07078 form is needed, it may be requested through the Access Control Unit, Production and Operations, Office of Information Services.

CLICK [HERE](#) to acknowledge that you have read, understand, and will comply with this policy.

VII. APPENDIXES:

- A. SUBJECT MATTER EXPERT
- B. ODJFS Code of Responsibility, [JFS 07078](#)

Owning Entity	Address	Name (SME)	Phone/ Fax/ E-mail
OIS	4200 E. Fifth Ave. Columbus, OH 43219-2551	Rick Copley, ODJFS Chief Security/Privacy Officer	614-466-2303 (OIS) 614-387-8126 (desk)

Exhibit 2

Page 4 of 4

			614-752-6815 (fax) ODJFS_Security@jfs.ohio.gov
OIS	4200 E. Fifth Ave. Columbus, OH 43219-2551	James Matheke, Information Security Architect	614-466-2303 (OIS) 614-387-8935 (desk) 614-752-6815 (fax) ODJFS_Security@jfs.ohio.gov