Ohio | Department of Job and Family Services

OIS Service Level Agreement
FY 2012-2013
Version 6.0

SLA.03 Information Security

ODJFS and County Agency Users have access to a great deal of personal information about our clients. ODJFS and County Agencies are required to safeguard the private information of our clients and staff. This section of the SLA gives the requirements for information security for all users of the ODJFS network.

3.1 General Information

3.1.01 *Information Security Policy*

Description	L1	L2	L3	LN
Create and maintain *Information Security Policy*	S	S	S	S

The ***Information Security Policy*** (IPP.3001) is administered by the ODJFS OIS *Access Control* Unit. The policy is available on the InnerWeb by clicking on the “Internal Policies” located on the InnerWeb home page under popular links or it is available in the Site Index.

In the event of a conflict between the information presented here and the information on the InnerWeb site, the InnerWeb site prevails. A county agency may also create and maintain its own *Information Security Policy* in addition to the ODJFS policy. However, in all situations the ODJFS *Information Security Policy* takes precedent over any county *Information Security Policy* in regards to ODJFS systems, except when the county policy is more restrictive.

Information for County Agencies is contained in **SLA.02 User Rights and Responsibilities**, which should be read in conjunction with this section.

3.1.02 Comply with IPP.3001 *Information Security Policy*

Description	L1	L2	L3	LN
All users of the ODJFS network or systems shall comply with IPP.3001 *Information Security Policy*	B	B	B	B

The *Information Security Policy* has been developed over time with input from federal agencies, county agencies, industry best practices, and ODJFS specific requirements relating to privacy. Failure to comply with the policy may lead to disciplinary action and loss of access.

3.1.03 Knowledge Transfer to Local Security Coordinators and Technical Points of Contacts

Description	L1	L2	L3	LN
Knowledge transfer to Local Security Coordinators (*LSC*) and Technical Points of Contacts (*TPOC*)	S	S	S	S

ODJFS OIS provides knowledge transfer for *LSC*s and *TPOC*s, either on an as needed basis, as part of a software deployment or as part of the annual *TPOC* Skills assessment training.

3.1.04 Apply for Network/System User IDs

Description	L1	L2	L3	LN
Complete the Code of Responsibility form (JFS 7078) to apply for Network/System User IDs	C	C	C	C

County Employees - The County Employee along with their supervisor and/or the *LSC* will complete the Code of Responsibility form, sign it, and then send it to *Access Control* with a detailed cover memo.

County Contractors - The County Contractor along with the county supervisor and/or the *LSC* will complete the Code of Responsibility form, sign it, and then send it to *Access Control* with a detailed cover memo. The supervisor and/or *LSC* must provide the contractor's company name and telephone number on the form.

External Entities - Request for access should be made utilizing the External Entity- VPN User Registration process. This process requires 2 forms; 1-ODJFS VPN Application for External Entities form (JFS 01320), Code of Responsibility form (JFS 07078). Both forms should be submitted through TSSP.
The External Entity - VPN User Registration Process instructions and forms can be found at: http://innerweb/omis/InfoSecurity/VPN_token_-_External.pdf

3.1.05 Correct User Login/Logout

Description	L1	L2	L3	LN
Ensure Users login/logout correctly	C	C	C	C

The *LSC* and *TPOC* shall jointly ensure that county agency users are aware of the login and logout procedures. An unattended "logged-on" computer is a security risk. The *LSC* and *TPOC* have the primary responsibility for ensuring that users know how to login and logout correctly to protect the confidentiality, integrity, and availability of data. The *LSC* and *TPOC* have a responsibility to ensure county agency users know how to lock the PC and how to login & logout correctly to prevent data loss and *workstation* corruption. Please refer to the **User Responsibilities** section contained within **IPP.3001 *Information Security Policy*** for more detailed information.

3.1.06 Password Resets

Description	L1	L2	L3	LN
Understand password reset responsibilities and policy	CO	C	C	C

ODJFS policy states that *password* resets should be performed at the County Agency level for efficiency and security reasons. Subsections 3.1.07 through 3.1.08 specify *password* resets according to type of system.

If an SLA level 1 County Agency does not want to perform their own *password* resets, the ODJFS OIS Service Desk can provide this service.

In an emergency, due to the event that the primary *LSC* and secondary *LSC* are not available any *TPOC* or *LSC* can contact the OIS Service Desk to provide *password* resets, but only after verification of identification of those who are requesting a *password* reset.

3.1.06.a *Mainframe* (IBM) Passwords and Lockouts

Description	L1	L2	L3	LN
Perform *mainframe* (IBM) *password* resets and clear lockouts	CO	C	C	C

*LSC*s and *TPOC*s have the option to reset their county agency users' *password*s and clear lockouts on the IBM *Mainframe*. If an *LSC* or *TPOC* does not have this access and would like to have this ability, the Agency Director or current primary or secondary *LSC* must send a Code of Responsibility (JFS 7078) form to *Access Control*. The request should include the RACF User ID and specify they are requesting TSO *password* reset capabilities.

Access Control will grant this access and send training instructions to the individual and *LSC*. If the individual would like to set up a training phone conference, this can be arranged as well by sending a request to *Access Control*.

3.1.06.b Novell Passwords and Lockouts

Description	L1	L2	L3	LN
Perform Novell password resets and clear lockouts	CO	C	C	C*

*LSC*s and *TPOC*s have the option to reset their county agency users' Novell *password*s and clear lockouts by using Novell's iManager. If an *LSC* or *TPOC* does not have this access and would like to have this ability, the Agency Director or current primary or secondary *LSC* must send a Code of Responsibility (JFS 7078) form to *Access Control*. The request should include the Novell User ID, and specify they are requesting Novell *password* re-set capabilities.

Access Control will grant this access and send training instructions to the individual and *LSC*. If the individual would like to set up a training phone conference, this can be arranged as well by sending a request to *Access Control*.

3.1.07 User IDs

Description	L1	L2	L3	LN
Granting, modifying and terminating of Users IDs, including name changes.	S	S	S	S

The *LSC* requests *Access Control* to grant, modify or terminate county agency users, including name changes. Sections 3.1.10 through 3.1.15 detail how to request modification and removal of User accounts. Please see the *Access Control* web page for the appropriate forms and to ensure proper procedures are followed.

3.1.08 Granting and Terminating Access of User IDs

Description	L1	L2	L3	LN
Granting and terminating User IDs	S	S	S	S

The *LSC* requests new access via the Code of Responsibility (JFS 7078) form. Once *Access Control* has created the user's ID and granted the approved level of access, confirmation is sent to the *LSC*. The *LSC* then will build a (CRISE,SETS or SACWIS) profile if necessary and assist their user with logging into the system.

The *LSC* requests deletion of a county agency user's ID directly to *Access Control*. The *LSC* must include the person's first and last name, User ID, last day of employment, and list all known accesses. It is the *LSC*'s responsibility to end-date and inactivate all CRISE and SETS profiles prior to sending notification to *Access Control*.

The *LSC* can also request proxy access to the terminated county agency users' P:(personal) drive and GroupWise email for a period of one month.

3.1.09 *Mainframe* (IBM) and Novell Disable User IDs

Description	L1	L2	L3	LN
Perform *Mainframe* (IBM) and Novell disable of User IDs.	B	B	B	B

The *LSC* has the option to disable their County Agency User's Novell and *Mainframe* IDs. Once the account is disabled by the *LSC*/*TPOC*, *Access Control* must be notified. *Access Control* needs to review and terminate accesses for the individual into other systems (i.e. VPN, SCOTI, SACWIS, etc.).

The ability to disable a *Mainframe* and Novell User ID is granted when requesting the ability to reset and clear intruder lockouts. *Access Control* will grant access and send training instructions to the *LSC* via GroupWise email. If the *LSC* would like to set up a training phone conference, this can be arranged by sending a request to *Access Control*.

If the *LSC* chooses not to have these abilities, they will send disable requests to *Access Control*.

Complete termination instructions can be found on *Access Control*'s Webpage: http://innerweb/omis/InfoSecurity/InfoSecindex.shtml

3.1.10 Change Name and User ID

Description	L1	L2	L3	LN
Process for a Name and/or User ID Change.	S	S	S	S

If a User's name legally changes and would like their name changed on ODJFS systems, a request should be sent to *Access Control*. The request should include the County Agency, User's former name & user ID and their new desired name. *LSC* can notify ODJFS of name change using the On-Line name change form located on *Access Control*'s webpage. Once the name has been changed the *LSC* will be notified with the User's new user ID.

Please note a User's *mainframe* user ID never changes. It is up to the *LSC* to change the users name on their SMUM (Security Maintenance/User Maintenance) profile.

3.1.11 Change User information

Description	L1	L2	L3	LN
Change User information, including address, title, and phone number changes, in directory services.	C O	C	C	C

All individuals have the ability to update their own phone, fax, cell number, address, and title within GroupWise using eGuide. If a person has difficulty or is unable to update this information, the *LSC* can make these changes for the person. If the *LSC* has difficulties, ODJFS OIS can provide this service.

The *LSC* has the option to update their County Agency User's phone, fax, and cell number, address, and title within GroupWise using Novell iManager. If an *LSC* does not have this access and would like to have this ability, the Agency Director or current primary and/or secondary *LSC* must send a 7078 Code of Responsibility form to *Access Control*. The request should include the Novell User ID and specify they are requesting Novell eGuide capabilities.

Access Control will grant the access and send training instructions to the *LSC* via GroupWise email. If the *LSC* would like to set up a training phone conference, this can be arranged as well by sending a request to *Access Control*.

3.1.12 Position Changes

Description	L1	L2	L3	LN
User Move/Position changes	S	S	S	C

When a county agency user's position or role changes at the county, their current access need to be reviewed and changed based on the needs of the new position. Please see the *Access Control* Web page "Moves/Position Changes" for the necessary forms and procedures.

3.1.13 File Shares and Group Rights Assignments

Description	L1	L2	L3	LN
New or Modified File Share folders and Group Rights Assignments	S	S	C	C

The State maintains creation of shared folders and associated groups for SLA level 1 and 2 County Agencies. Anytime a change is needed for a county agency's shared folders and associated groups a request should be sent to the OIS Service Desk to request the change. The OIS Production Administrators make the requested modification. SLA level 3 County Agencies control their Agency's shared files and group rights assignments.

3.1.14 File Shares and Group Membership Rights

Description	L1	L2	L3	LN
Group Membership Modifications	S	CO	C	C

Upon request from the County Agency director an SLA level 2 *LSC* can be granted rights to modify group membership for their agency. However, the state controls the creation of folders and groups.

3.1.15 ODJFS Reconciliations reports

Description	L1	L2	L3	LN
ODJFS Creates reports for Local Security Coordinators to review	S	S	S	S

As part of ongoing operations, periodic reviews are conducted to clean up inactive and duplicate user accounts. User ID's that have not been logged into in a 90 day or greater period will be disabled and reviewed. Duplicate accounts are not permitted on any ODJFS systems. *Access Control* creates and emails reports on a regular basis to county mailboxes for the *LSC*'s to review, in accordance with IPP 3930 Periodic Access Reconciliation.

- Monthly spreadsheet – list of Novell accounts that have not been logged in to the ODJFS Network for over 90 days.
- Quarterly spreadsheet – list of Novell accounts that have been disabled but have not been deleted
- Yearly spreadsheet – list of Novell accounts to review

3.1.16 Review Reconciliation reports of User IDs

Description	L1	L2	L3	LN
Review reconciliation reports and communicate changes to the *Access Control* unit.	C	C	C	C

According to IPP.3930 Periodic Access Reconciliation process, *LSC*'s are the main point of contact with the *Access Control* Unit on all security issues. To ensure access to ODJFS application and data remain secure, OIS and Program Data owners have implemented a reconciliation process which requires timely communication of user's access. The county *LSC* should review reports sent to county mailboxes and report back to *Access Control* on user accounts that require modification, revocation or removal.