Ohio | Department of Job and Family Services

OIS Service Level Agreement
FY 2012-2013
Version 6.0

SLA.02 User Rights and Responsibilities

This User Rights and Responsibilities section governs proper use of ODJFS owned equipment, county agency owned equipment, and the ODJFS network. It is intended for the use of all county agency employees. County agency employees must comply with responsibilities outlined in this section to ensure the proper operation and maintain the security of the ODJFS network. County agency employees should refer to the **User Responsibilities** section contained within **IPP.3001 *Information Security Policy*** for additional information on the responsibilities delineated in this section. All ODJFS Internal Policies including IPP.3001 *Information Security Policy* can be found on the ODJFS Innerweb located under popular links.

2.1. General Information

2.1.01 Security Policy

Description	L1	L2	L3	LN
Comply with ODJFS IPP.3001 *Information Security Policy*	C	C	C	C

Network security is critical to the success and efficiency of ODJFS provided applications. Every network user is expected to understand and comply with the ODJFS *Information Security Policy*.

2.1.02 Login/Logout Procedures

Description	L1	L2	L3	LN
Comply with login/logout procedures	C	C	C	C*

The County Agency is responsible to ensure that employees are aware of the login and logout procedures. This ensures consistent access for authorized users, prevents unauthorized access to the ODJFS network, and assures timely receipt of centrally distributed software to the desktop. All County Agency employees must comply with these procedures. Please refer to the **User Responsibilities** section contained within **IPP.3001 *Information Security Policy*** for more detailed information.

NOTE: County Agency employees must lock their PCs during the day whenever they leave the PC. County Agency employees must log off their PCs at the completion of every work day to

ensure all files are successfully backed up. A complete backup of all system files cannot be performed if an employee has not closed all open files and is logged off their computer. Any file that remains open cannot be efficiently backed up. This includes, but is not limited to, spreadsheets, word processing files, databases, etc.

2.1.03 Passwords

Description	L1	L2	L3	LN
Comply with no sharing of User IDs and *password*s	C	C	C	C

There is to be no sharing of individual User IDs and *Password*s under any circumstances as referenced in the Internal Policies and Procedures Manual IPP.3922 Code of Responsibility. *Password*s must be at least six characters (8 characters preferably) in length. The *password* should be a combination of alphabetic and numeric characters.

2.1.04 Name Changes

Description	L1	L2	L3	LN
Notify *LSC* of user name changes, *LSC* to contact *Access Control*	C	C	C	C

All County Agency employees who change their legal name must contact the *LSC* and inform him or her of the change. The *LSC* will contact *Access Control*, with the change information. The *LSC* will inform the user when the change is complete.

2.1.05 Internet Use

Description	L1	L2	L3	LN
Comply with Internet Use Policy	C	C	C	C

All county agency employees must comply with the Internet Use Expectations found in IPP.3001 *Information Security Policy* and ODJFS Internet Access Guidelines as referenced in IPP.10002 Computer and Information Systems Usage except when the County Agency policy is more restrictive.

In accordance with the Internet Access Guidelines, the County Agency Director may request the monitoring of county agency user's Internet usage. These requests should be submitted to the ODJFS Chief Inspector's Office by calling 614/466-3015 or via the following link http://innerweb/oci/

2.1.06 Anti-virus Tools

Description	L1	L2	L3	LN
Comply with compulsory use of anti-virus software	C	C	C	CO

SLA Level 1, 2 and 3 County Agencies must use all ODJFS provided anti-virus software. SLA Level 1 and 2 County Agencies may not modify the settings for any ODJFS provided anti-virus software. An SLA Level 3 County Agency may modify the settings for ODJFS provided anti-virus software as long as the modifications increase the level of virus protection provided. All County Agencies must also provide up-to-date anti-virus software for any County Agency equipment connected to the ODJFS network. County agency equipment found not in compliance is subject to immediate disconnection without prior notice. The anti-virus software must automatically scan upon boot-up on a weekly basis to check for and clean any infected files.

2.1.07 *Licensing*

Description	L1	L2	L3	LN
Purchase sufficient *licensing* for all non-ODJFS standard software on County Agency or ODJFS owned equipment	C	C	C	C

In accordance with the IPP.3001 *Information Security Policy*, the County Agency may not load any software on to ODJFS network equipment that has not been authorized via the TSSP process and must not violate any copyright laws. The County Agency must purchase sufficient *licensing* for all non-ODJFS standard software deployed in the County Agency. In addition, County Agency users should refer to IPP.3440 Software Copyright Compliance Policy for additional guidance on the responsibilities related to software compliance.

In accordance with TSSP, the County Agency may not load any non-ODJFS standard software onto ODJFS network equipment without first obtaining written approval from ODJFS OIS. Requests for approval should be made through the TSSP process. ODJFS may perform periodic inventory scans to verify compliance with the *licensing* provision of SLA.

2.1.08 Drive Space

Description	L1	L2	L3	LN
Comply with network drive space usage.	C	C	C	NA

County Agency users must comply with the use of network storage and drive mapping standards as referenced in IPP.3942. Network *drives* allow users to access shared drive space and may eliminate the need to store data directly on the *workstation* hard drive. ODJFS may perform periodic inventory scans to verify compliance with the use of shared *drives*.
An SLA Level 3 County Agency will monitor its own drive space usage. If business needs require additional drive space for a user the County Agency should contact the OIS Service Desk at 1-800-686-1580.

2.1.09 Non-business Related Materials

Description	L1	L2	L3	LN
Refrain from storing non-business related materials on any drive	C	C	C	C

County Agency employees should refrain from storing any non-business related material on any local or network drive as is referenced in IPP.10002 Computer and Information Systems Usage. All data stored on the local and network *drives* is ODJFS property and subject to inspection if the County Agency or ODJFS deem necessary. Please refer the *Information Security Policy* and IPP.10002 Computer and Information Systems Usage for more detailed information.

2.1.10 Streaming Audio and Video

Description	L1	L2	L3	LN
Comply with restricted use of streaming audio and video unless authorized as official business.	C	C	C	C*

County Agency users must comply with the restricted use of streaming audio and video. Unauthorized streaming audio and video slows network response times for state supplied applications and could introduce unwelcome and costly viruses to the ODJFS network. If necessary, the County Agency *TPOC* can submit a TSSP form to request that unauthorized streaming audio and video be blocked from their site.

.