500		
LOUISIANA DSS Department of Social Services	**Agency Name**	Office of Family Support (OFS)
	Chapter No./Name	00. Miscellaneous Issuances Manual
	Part No./Name	E. Executive Bulletins
	Section No./Name	E-2500 Executive Bulletins
	Document No./Name	E-2567-00 Safeguarding Federal Tax Information
	Effective Date	January 15, 2017

SAFEGUARDING FEDERAL TAX INFORMATION

This Executive Bulletin is being issued to provide awareness about safeguarding federal tax information (FTI). To determine agency compliance with the Internal Revenue Services Security Guidelines, the IRS conducts an onsite review every three years. In a review conducted on January 29-31, 2008, several deficiencies were identified in regard to securing, maintaining, and storing federal tax information.

To insure that this agency maintains its authorization to access FTI, all DCFS employees and contractors with access to FTI are responsible for safeguarding this information, reviewing Publication 1075 - Tax Information Security Guidelines for Federal, State and Local Agencies and signing an IRS Tax Information Confidentiality Statement at least annually.

The following guidelines were added to Publication 1075 in August, 2010:

9.18.3 Remote Access

Accessing databases containing FTI from a remote location, i.e., a location not directly connected to the Local Area Network (LAN), will require adequate safeguards to prevent unauthorized entry. The IRS policy for allowing access to systems containing FTI is outlined below:

- Authentication is provided through ID and password encryption for use over public telephone lines.
- Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.
- Standard access is provided through a toll-free number and through local telephone numbers to local data facilities.

Both access methods (toll free and local numbers) require a special (encrypted) Page 58 modem and/or Virtual Private Network (VPN) for every workstation and a smart card (microprocessor) for every user. Smart cards should include all identification, authentication, and data encryption features. Two-factor authentication is required whenever FTI is being accessed from an alternate work location or if accessing FTI via the agency's web portal.

9.18.4 Internet

Federal, state, and local agencies that have Internet capabilities and connections to host servers are cautioned to perform risk analysis on their computer system before subscribing to their use. Connecting the agency's computer system to the Internet will require that adequate security measures are employed to restrict access to sensitive data.

9.18.5 Electronic Mail

Generally, FTI should not be transmitted or used on the agency's internal e-mail systems. FTI must not be transmitted outside of the agency, either in the body of an email or as an attachment. If transmittal of FTI within the agency's internal e-mail system is necessary, the following precautions must be taken to protect FTI sent via E-mail:

- Do not send FTI unencrypted in any email messages.
- The file containing FTI must be attached and encrypted.
- Ensure that all messages sent are to the proper address.
- Employees should log off the computer when away from the area.

9.18.6 Facsimile Machines (FAX)

Generally, the telecommunication lines used to send fax transmissions are not secure. To reduce the threat of intrusion, observe the following:

- Have a trusted staff member at both the sending and receiving fax machines.
- Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI.
- Place fax machines in a secured area.
- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient. This includes:
    - A notification of the sensitivity of the data and the need for protection.
    - A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.

Safeguarding guidelines of restricted information are available in SES C-700, DSS 5-03, DSS 5-03-13, DSS 5-03-17, DSS 5-03-19, and DSS 5-03-24.

A complete list of guidelines is available in Publication 1075.

Additional DCFS Security policies are available: DSS 5-03-3 Awareness and Training, DSS 5-03-10 Password Management, DSS 5-03-11 Incident Response, and DSS 5-03-17 Acceptable Use.