

Early Learning Coalition of Florida's Heartland, Inc.

Attachment 1.1.12 and 1.1.13

Subject: Confidentiality of Data; Electronic Transmission of Confidential Data		Policy/Procedure # FM-8	
Page: 1 of 4		Adoption Date: 8.22.07	Revision Date:
Approved by: ELCFH Board		Title: Andrew Bible, Chair	
Distribution: Upper Administrative staff; Finance staff		Authority References: Executive Director, Finance Officer	

References:

- s. 1002.72, F.S.
- s. 411.011, F.S.
- Chapter 119, Florida Statute
- AW Policy Number 5.02

Purpose: To ensure confidential Coalition data is maintained and transmitted securely.

Background: AWI requires Early Learning Coalitions establish protocols to ensure all confidential data is maintained and transmitted appropriately and securely.

Policy:

All Coalition Staff share the responsibility of protecting the Coalition's information resources and adhering to the policy regarding their usage.

Maintenance of Confidential Data

- The Coalition and its partnering agencies who receive early learning records in order to carry out official functions protects the data in a manner that may not permit the personal identification of children or their parents by persons other than those authorized to receive the records;
- Requests for review of public documents must be submitted in writing to the Executive Director. Copies may be furnished at \$1 per page to cover copying and labor costs. The Executive Director will review any documents before releasing to ensure no client data or other confidential data is disclosed.

Transmission of Confidential Data

The Coalition must safeguard confidential data such as names and addresses, social security numbers, and federal employment numbers. Unencrypted transfer of confidential information by email is

♡ Charlotte Office
3028 Caring Way, Suite 4
Port Charlotte, FL 33952
Phone: 941 255-1650
Fax: 941 255-5856
Toll-Free: 866-639-4979

♡ DeSoto Office
4 West Oak Street, Suite H
Arcadia, FL 34266
Phone: 863 494-5233
Fax: 863 494-5291
Toll Free: 866-639-4979

♡ Hardee Office
324 N. 6th Avenue
Wauchula, FL 33873
Phone: 863-767-1002
Fax: 863-767-1007
Toll Free: 866-639-4979

♡ Highlands Office
209 N. Ridgewood Drive
Sebring, FL 33870
Phone: 863-314-9213
Fax: 863-314-4480
Toll-Free: 866-639-4979

prohibited as e-mail transmission of data is not secure. This prohibition applies to submissions to AWI.

Examples of secure transfer of confidential data include but are not limited to the following:

- Encrypt file with applicable software.
- Use last names plus the last four digits of social security numbers.
- Fax only if the transmission is to a secure location and picked up immediately.
- Ensure that sensitive paperwork is secured.
- Transmit data behind a firewall.

Protocols:

Acceptable Use of Information Resources

Individuals using information resources belonging to the Government must act in a legal, responsible, and secure manner, with respect for the rights of others.

Information Resources Classification

All information resources (including data and systems) must be identified, categorized and protected according to their level of confidentiality and business “need to know”. All files should be stored and filed appropriately on the Share drive (S:\) of the Coalition server.

Security Training & Awareness

The Coalition’s information security policies, procedures and protocols shall be communicated to all employees, and shall be available for reference within the ELCFH Employee Handbook. Changes will be discussed at Coalition staff meetings.

Incident Reporting

Coalition personnel are required to report any suspected security incidents. Reports of suspected security incidents should be submitted to the appropriate Associate Director or Executive Director.

Incident Response

The Coalition must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

Security System Plans

The Coalition must maintain a firewall.

Contingency Planning

Alternate modes of operation exist to ensure continuity of critical services in the event of a natural disaster, fire, act of terror, or other catastrophic event as outlined in the Continuing Offsite Operations Plan.

Access Control

Access to Coalition information resources shall be limited to those that need them to perform their job duties. The principle of least privilege shall be applied to the allocation of access rights.

Identification and Authentication

Access to Coalition information systems shall only be granted to identified and authenticated users.

Antivirus

Standard software and procedures must be implemented to minimize the impact of computer viruses on the Coalition's information resources.

Physical and Environmental Security

Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft alteration, damage by fire, dust, water, power loss and other contaminants and unauthorized disruption of operation.

Change Control

All changes made to the Coalition's information systems shall be made in a controlled and coordinated fashion to preserve the confidentiality, integrity and availability of the system.

Backup and Recovery

Recoverable backups must be maintained for Coalition resources.

Patch Management and System Updates

Systems are to be maintained with updated security patches.

Server Security

Servers shall be made secure before placing them into the Coalition operational environment and security shall be maintained throughout their lifecycle.

Mobile Computing

Security controls shall be implemented to mitigate the increased risk posed by the use of laptops and other mobile devices outside of the Coalition office.

Network Security

Network devices and connectivity components shall be made secure before placing them into the Coalition operational informational technology environment, and security shall be maintained throughout their lifecycle.

Remote Access

Security controls shall be implemented to mitigate increased risks posed by allowing remote connectivity into the Coalition network.

Electronic Mail

Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise and business disruption.

Database Security

Information must remain consistent, complete and accurate.

Media Management

Media must be handled, stored and disposed of properly in order to protect the confidential Coalition data stored upon it.

Password Management

The Coalition shall protect access to its information resources by ensuring the any passwords used for authentication are properly assigned and protected.

Information Asset Management

All information assets must be tracked and managed to ensure that they are not lost or misused.