INFORMATION TECHNOLOGY SECURITY POLICY

PURPOSE

The purpose of this policy is to provide guidance for the security of all financial and confidential data and documents of the Coalition to ensure they are protected at all times. These guidelines establish minimum standards that must be upheld and enforced by users of the Coalition's technologies and communications system.

SCOPE

This policy applies to all employees of the Coalition, its contractors, vendors and agents with a work-station connected to the Coalition network or Enhanced Field System (EFS) database.

POLICY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected personal information and that access to sensitive information is restricted to authorized users.

The Coalition shall implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users only.

All employees, contract employees, vendors and others who have a business relationship with the Coalition are expected to comply with the provisions of this policy.

DEFINITIONS

Confidential Records - refers to entire record systems, specific records or individually identifiable data that by law are not subject to public disclosure under Article I, Section 24 of the Florida Constitution and Chapter 119, F.S. When applicable, confidentiality covers all documents, papers, computer files, letters and all other notations of records or data that are designed by law as confidential. Further, the term confidential also covers the verbal conveyance of data or information that is confidential. These confidential records may include but are not limited to, social security numbers, parent and child information, payment, child care provider, household demographics and resource and referral, which are private and confidential and may not be disclosed to others.

Personally identifiable information (PII) – any data that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.).

Security Incident – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with Coalition operations.

Breach of Security – unauthorized access of data containing personal information. Good faith access of personal information by an employee of the Coalition does not constitute a breach of security, provided the information is not used for a purpose unrelated to the programs.

PROCEDURE

1. Security Training and Awareness
   The Coalition shall require all employees to receive security training and awareness information upon hire. Completion of the data security training shall be evidenced by the signing of Florida's Office of Early Learning Data Security Agreement.

2. Identification and Authentication
   a. To ensure only authorized individuals have access to confidential information, the Coalition has established the use of computer usernames and passwords to limit access and restrict use of individual employees' computers, based on the established user identity.
   b. The Coalition's IT contractor shall establish and store all records of usernames and passwords. Should access be needed to a Coalition computer, the IT contractor shall delete and restore the username and password information to allow entry under a new username and password.
   c. Each employee's username and password shall allow them to gain access to only those software and data files necessary to perform their assigned duties.
   d. Upon an employee's resignation or termination, the Coalition shall immediately contact the IT contractor to delete the employee's computer access and provide access to the Coalition for information retrieval.

3. Access Controls
   a. The confidentiality and integrity of data stored on Coalition computer systems shall be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only access appropriate to each employee's job duties.
   b. Employees assume all responsibility for their access to the Coalition's information system. Usernames and passwords must not be shared with others. Usernames and/or passwords shall only be provided in cases necessary to facilitate computer maintenance and repairs and then only to authorized Coalition staff or authorized contracted IT personnel. Unauthorized access to the Coalition's information system is prohibited.
   c. To further ensure data security, inactivity time-outs are automatically programmed to occur on each workstation after thirty (30) minutes of inactivity.
   d. Employees receive and sign a Data Security Agreement upon hire and annually thereafter.
   e. Requests for new employee accounts or closing accounts are handled by the Office Manager or Assistant Executive Director as needed based on system/access required. New account information and closed account information will be maintained in the employee file.
   f. Closed account procedures include the following:
      - Removal of access privileges and computer accounts.
      - Return of any information resources (property or data).

4. Password Management
   a. Network passwords shall contain at least nine (9) characters and must consist of a combination of

letters, numbers and special characters.

b. Network passwords must be changed every ninety (90) days.

c. Password management complies with requirements for passwords described in OEL's IT Security Policy.

5. Mobile Computing

All laptop computers will be username and password protected to ensure data security. These computers may only be checked out to designated employees of the Coalition. A log will be kept to effectively track the location and use of these computers.

6. Remote Access

Remote access is provided to a limited number of staff. Log records are maintained on all workstations and firewall logs are monitored for unusual activity by the IT contractor.

7. Records Confidentiality Compliance

a. All information subject to confidentiality about clients, children or other confidential information, shall not be shared with any unauthorized person in or outside the Coalition without prior written approval of the individual, family or the Coalition, as applicable.

b. The use of personal devices to download or store sensitive or confidential information is prohibited.

c. The use of mobile computing devices that are uncrypted or lack activated password protections are prohibited.

8. Personnel Security

a. Upon hire, all employees shall be given the IT policy for review to ensure a thorough understanding of data security within the Coalition. All employees shall complete a data security training, as evidenced by the Data Security Agreement, which is signed after completion of the training.

b. Should an employee resign or be terminated, all files on the Coalition's computer shall become the property of the Coalition. Additionally, the employee's user account information is inactivated immediately.

c. The Coalition's IT contractor shall be required to sign a Data Security Agreement.

9. Breach of Security

The Coalition will notify OEL in writing of any security incident or breach of security by its employees or representatives in writing within 24 hours of learning of the incident or breach. The notification will include the nature of the incident, the confidential information used or disclosed, who made the unauthorized use or received the unauthorized disclosure, what the Coalition has done to mitigate the incident, and any corrective action the Coalition has put in place to avoid another incident of this type.

10. System Monitoring/Anti-Virus Protection

a. The Coalition, in conjunction with its IT Contractor, will monitor the adequacy of system hardware, performance and capacity-related issues on a monthly basis. (Detailed information available under Scope of Services within the IT Services Contract.)

b. The IT Contractor is responsible for the following:

- Updating antivirus and anti-malware software.
- Performing services necessary to eliminate files if spyware and viruses are detected.
- Verifying antivirus definition date to ensure all scheduled updates have been performed properly and effectively.

- Deleting all quarantined files to rid workstation of known viruses and identify files that could be potential problems.
- Performing a scan disk on each computer and document any anomalies.
- Reviewing the event log to determinate any potential problems.

11. Data BackUp
Coalition data is backed up daily and stored in a fireproof safe on site. The IT Contractor reviews backup tapes to ensure backups are accurate. The Coalition reviews all policies and procedures annually to identify any areas for change/update.

12. Physical and Environmental Security
The Coalition complies with requirements set forth in OEL IT Security Policy 5.05.02.17 to ensure there is limited physical access to network system wiring closets and other computer storage areas and confidential information resources (i.e., servers, backups, etc.)

13. Computer Equipment Disposal
The Coalition, in conjunction with the IT Contractor, will ensure any/all entity data, sensitive client or operational data, etc. are removed prior to disposal.

Applicable Authoritative Citations: (Additional information can be found in OEL Grant Agreement)
2 CFR 200.335, *Methods for collection, transmission and storage of information*
OEL IT Security Manual
OEL Program Guidance 101.02, *Records Confidentiality*
Computer-related Crimes, Chapter 815, F.S.
1002.84(13), F.S.

Approved:
Board of Directors – July 23, 2015
Revisions Approved by Executive Committee:
June 15, 2016