Children's Services Council of Leon County

POLICY: Data and System Security
Adopted February 2, 2023

CSC Leon recognizes the importance of maintaining the security of data and technology resources required to operate the organization and provide accurate reporting on outcomes. All individuals who collect participant data, specifically that which contains personally identifying information (PII), should take reasonable measures to protect and secure it, both in written and electronic formats.

CSC Leon will be responsible for the following:

- Training administrators of Community Investment Partners (CIPs) on acceptable measures to ensure data security within their program(s).
- Limiting user access to only data that required to perform their specific job duties.
- Regularly auditing file access permissions.
- Implementing procedures to report data breaches or violations of security protocol.
- Educating program administrators on any new developments in data breach security.
- Implementing disposal standards for participant data no longer subject to be retained in accordance with CSC Leon policies nor Florida's public records law.

Administrators for CIPs will be responsible for the following:

- Communicating with CSC Leon, in writing, the names and positions of all persons who should be authorized to access data files and system modules within the CSC Leon Services & Activities Management Information System (SAMIS).
- Notifying CSC Leon of any change in personnel or their authorization to SAMIS.
- Training employees within CIPs on steps to take to ensure data security as part of their program duties.

All users of the CSC Leon SAMIS in any capacity will be responsible for the following:

- Reporting suspected or actual data breaches immediately to either the CSC Leon Special Projects Manager or Executive Director. Examples of the types of incidents to report include, but are not limited to:
  - Access to system data files or modules by unauthorized individuals;
  - Evidence of unauthorized access into a system containing private/confidential data;
  - Unauthorized sharing of login credentials;
  - Loss of a hardware resource such as laptop, tablet, cell phone, or removable data storage devices;
  - Hacking or defacing of an online resource within the information management system;
  - Documents containing private/confidential data sent in any form to a wrong recipient;
  - Employee misuse of authorized access to disclose or mine private or confidential data.
- Protect all data files and system modules by signing off the system or locking their equipment/office while unattended.

Activating Incident Response Team

Upon receipt of a suspected information security breach, the CSC Leon Special Projects Manager, Executive Director, or designee will immediately contact Webauthor and expeditiously conduct a fact-finding investigation to determine whether a data breach or compromise has occurred.

If the team determines there was a data breach, appropriate resources will work to contain the breach. Once the breach is contained and eradicated, the team will assess the extent and impact of the breach. Each step related to the breach and breach investigation will be fully documented.

The team will consult with legal counsel to determine specific legal obligations relating to the breached information and relevant reporting obligations such as:

- Family Educational Rights and Privacy Act (FERPA);
- Health Insurance Portability and Accountability Act (HIPAA);
- State of Florida laws;
- Federal laws including the Federal Trade Commission Act and Gramm-Leach-Bliley Act;
- Any relevant contractual obligations

If a data breach compromise protected personal information of over 500 individuals in the State of Florida, CSC Leon must inform the Florida Department of Legal Affairs as well as each affected or likely affected resident within 30 days of the breach. Additionally, CSC Leon in collaboration with Webauthor, will be required to make certain materials available to the state government upon request, such as remedial procedures, incident reports, and computer forensic.

Authorized Users and Passwords

Authorized users of CSC Leon's technology resources shall have passwords to authenticate their identity and provide access to the appropriate systems. Authorized users include CSC Leon team members and specific individuals within funded programs.

A. Appropriate persons may be properly authorized to access information management system data files and system modules, only if such operation is clearly a part of, or directly related to, the administrative workload of that individual. In all cases they must be properly authorized (i.e. have a signed and approved security user-id agreement) when access is permitted.

B. Program participants, volunteers and non-program staff should not be provided access to confidential information management system data files and system modules. Any exception will require prior approval of CSC Leon.

C. CSC Leon shall supply each duly authorized user with a unique user identification code and password to enable the user to sign on to the network.

D. All users will be required to update system passwords at least once every sixty (60) days. Passwords will be assigned by the information management system so that no one can find a

password in the system. If a password is forgotten a valid member can use the built-in tools to have a new, temporary password mailed to their valid member E-mail address and then using the temporary password they can log into the site and select a new password that is then hashed in the system. This and other measures that are built into "User/Member Administration" assure the highest level of application-level security. Multi-factor authentication may be required. Training for program administrators and data entry staff will be provided by CSC Leon.

E. CSC Leon minimum secure password requirements are:

1. Passwords will be at least eight (8) characters, with three (3) out of four (4) of the following conditions met:

    a. must contain an uppercase letter;
    b. must contain a lowercase letter;
    c. must contain a special character;
    d. must contain a number.

2. The password should be changed on a regular basis and at least once every sixty (60) days where there is significant risk relating to personally identifiable confidential information being accessed.

3. Screen saver and session time-outs and monitor orientation should be set to preclude casual screen viewing by others.

F. It is a violation for any person to disclose any assigned password to any other person, except to a member of the Webauthor team or their designee, for problem resolution purposes. It is the responsibility of each user to whom a password is assigned to maintain the confidentiality of the password. Under no circumstances shall passwords be posted or kept in a place that is accessible to unauthorized persons.

G. In general, users shall not be given access to system development and productivity tools. Specific exceptions may be made which may place additional restrictions on such access on an individual basis. Unauthorized access to program libraries and program development tools shall be considered a violation.