Policy: Security-User Responsibility

ChildNet Number: CN 012.015
Original Approved Date: June 5, 2003
Policy Revised Date(s): July 15, 2008; March 15, 2010
Policy Sunset Date:
COA Standard(s): RPM 5.01, 5.02, 6.01

Statement of Policy:

This policy establishes the Management Information Systems (MIS) security safeguards that must be taken by every person using ChildNet's resources or otherwise accessing Department of Children and Families (DCF) information. Additional safeguards may be appropriate, depending on the situation and its inherent risk to ChildNet's and DCF's resources.

Scope:

All of ChildNet's physical and intellectual assets as well as related stakeholder resources will be protected by the implementation of the necessary safeguards.

Board Chair's Signature: _____ **Date:** 11/5/10

Procedure: Security-User Responsibility

ChildNet Number: CN 012.015
Original Approved Date: June 5, 2003
Procedure Revised Date(s): July 15, 2008; March 15, 2010; August 22, 2014, February 14, 2024
Procedure Sunset Date:
COA Standard(s): RPM 5.01, 5.02, 6.01

Definitions: None

Statement of Procedure

1. All ChildNet and contract provider employees are to be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. Fulfillment of security responsibilities is to be mandatory and violations may be cause for disciplinary action, up to and including dismissal, civil penalties, or criminal penalties under chapters 119, 812, 815, 817, 839, or 877, Florida Statutes, or similar laws.

2. All employees, including provider employees with access to data through computer-related media, must read and sign the ChildNet Security Agreement Form, which is consistent with DCF CF-114. This includes an acknowledgment of the requirement that all thumb drives used for storing or transporting sensitive or confidential information must be approved and provided by the ChildNet MIS department and must have encryption enabled.

3. This policy and procedure regulates the assignment and use of computer system user IDs and associated passwords and employee responsibilities when granted system access. Information sharing with selected employees is to be handled through other administrative methods. The sharing of passwords is prohibited. Documents created on Word, Excel, or Power Point, that contain confidential or sensitive information must be password protected. The communication of the password must be done via a separate email or other manual methods.

4. All ChildNet laptop computers must have the C: drive encrypted and the Basic Input Output System (BIOS) password feature activated by MIS. Employees are prohibited from storing laptop computers in their automobiles unattended or overnight. If necessary, for personal safety concerns, during a home visit a laptop may be placed in a locked trunk prior to arriving at the home visit location.

5. Electronic mail, which may contain confidential or sensitive information, must be strong encrypted during transmission to ensure proper security. This encryption

safeguards the contents of the emails, making them accessible only to the intended recipients who have the correct access. To further enhance the security of electronic mail, special email rules and alias assignments should be individually established, allowing for the secure sharing of electronic mail, special directories and network access rights can be used to share Word document files with one or more people, and server security features are available to give supervisors appropriate access rights to their employees cases, if required.

6. Employees should investigate and use the above referenced available methods for information and access sharing rather than sharing passwords. See CN 012.006 – Electronic Mail.

   A. Each ChildNet employee's supervisor is to provide a copy of the ChildNet Security Agreement Form to every employee who is granted access to data through the use of computer-related media (e.g. printed reports, microfiche, system inquiry, on-line update, or any magnetic media). The contract manager is to determine whether the provider should be granted access to data through the use of computer-related media. If access is granted, the contract manager is to provide a copy of this operating procedure and the ChildNet Security Agreement Form to the provider for its employees who are granted access.

   B. ChildNet determines who within their organization are to have access to client or otherwise confidential data. The provider's Data Security Officer is to distribute the ChildNet Security Agreement Form to each provider employee granted access to data through the use of computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media).

   C. All company and provider employees who have access to data must read and sign the Security Agreement Form and, if necessary, obtain clarification from a supervisor or designee. The contract provider is to identify an individual to function as its Data Security Officer. This Data Security Officer is to act as a liaison to ChildNet's security staff. The provider is to obtain signed security forms at least annually from each of its employees who have access to data. When a ChildNet contract specialist is notified by a provider that there has been a breach or potential breach of personal and/or confidential data, as required by their contract, the ChildNet Contract Specialist is to notify ChildNet's Security Officer the same business day. *Note: For multi-year contracts, new signed forms must be obtained from each provider employee upon their anniversary date of hire.*

   D. All company and provider employees must adhere to and by signing the form, acknowledge receipt of the minimum security requirements in the "Florida Computer Crimes Act" (Chapter 815, Florida Statutes). This also includes related company policy and procedures.

E. ChildNet and each provider is responsible for maintaining the signed forms for its employees who are granted access to data and will upon request present these forms to authorized company staff. ChildNet employee supervisors are to sign and forward the original copy to the Office of Talent Management to be maintained in the employee's personnel folder.

F. All ChildNet and provider employees are to retain a duplicate copy of the form and a copy of the "Florida Computer Crimes Act" (Chapter 815, Florida Statutes).

President's Signature: _____ **Date:** 04-02-24