Policy: Security of Data and Management Information Systems Resources

ChildNet Number: CN 012.013
Original Approved Date: June 5, 2003
Policy Revised Date(s): February 19, 2003, April 14, 2010, May 20, 2010
Policy Sunset Date:
COA Standard(s): RPM 5.01, 5.02, 6.01

Statement of Policy

It is the policy of ChildNet to protect the confidentiality, integrity, availability, and reliability of all Management Information Systems (MIS) resources used to support the needs of our clients and the mission of ChildNet. To accomplish this goal, the MIS staff implements and enforces a level of security which will provide for the protection of data and MIS resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside ChildNet. Federal or state laws, rules, regulations, policies and procedures governing the confidentiality of data are not superseded, abridged, or amended by this operating procedure.

Scope

This Information Security policy is intended to support the protection, control and management of the entirety of ChildNet's information assets, to encompass data and information that is:

- Stored on databases
- Stored on computers
- Transmitted across internal and external networks
- Sent by facsimile or other communications method
- Stored on removable media such as CD-ROMS, hard disks, flash drives tapes and other similar media

As such, this policy will create an accountable, secure and extensible framework around all Information Technology resources and activities under the care and control of Management Information Systems (MIS).

Board Chair's Signature: _____ **Date:** 11/15/10

Procedure: Security of Data and Management Information Systems Resources

ChildNet Number: CN 012.013
Original Approved Date: June 5, 2003
Procedure Revised Date(s): February 19, 2003, April 14, 2010, May 20, 2010, June 10, 2014
Procedure Sunset Date:
COA Standard(s): RPM 5.01, 5.02, 6.01

Definitions (If any):

Data - a collection of facts; numeric, alphabetic and special characters which are processed or produced by a computer.

Data Center(s) - for security purposes, any site designated as such by the Information Security Manager.
Departmental Data Processing Systems - this includes systems that are maintained and operated at the DCF Technology Center, and other departmental data processing sites.

Information Security Manager - the person designated by the President of ChildNet to administer the organizations' data and MIS resource security program.

MIS Resources - data processing hardware, software and services, supplies, personnel, facility resources, maintenance, training, or other related resources.

Input Sources - the media used to collect and record data that are subsequently transferred to an automated information system.

Local Application Software - local data processing software that is the responsibility of the individual using the software at that location.

Management Information Systems (MIS) - interrelated systems which provided for the electronic, soft and hardware, support for the operations of ChildNet information data systems..

Micro-sites - district data processing sites that are not large enough to be declared data centers, but represent a hub of processing, or contain a significant amount of data processing equipment and other MIS resources that, if lost, would result in an extreme hardship on ChildNet to achieve its goals.

Output Products - the media generated as a result of the processing of data by an automated information system.

Security Officer(s) - the person(s) designated by ChildNet's Information Security Manager, Program Administrator, or Systems Director to administer a security program.

Stand-Alone Equipment - stand-alone equipment is information processing equipment (e.g., PCs, LAN Servers, Unix Systems, and Windows Systems) which uses local application software and is not dependent upon a central data processing system.

System Owner(s) - the entity that owns the data and has the primary responsibility for decisions relating to a particular data processing system's specification and usage.

Statement of Procedure

System Security

1. ChildNet Technology Center.

    a. Each person who uses equipment to access the systems located or provided by ChildNet or access any ChildNet data by means of MIS resources owned purchased or leased by ChildNet is to have a unique personal identifier(s). The identifier(s) are to be assigned and controlled by a security officer. This identifier(s) are confidential. Prior to obtaining a personal identifier, the owner must sign the Security Awareness Form and be scheduled to attend a Security Awareness Training session.

    b. The identifier(s) will permit access to the data that the person has a need and right to know and control inquiry and update capabilities. This access is to be determined and authorized by the owner of the system. This initial minimum security measure is to ensure a general level of security across all systems. Additional levels of security may be implemented if deemed necessary and approved by the Security Officer.

2. Stand-alone Equipment. Security measures for systems on stand-alone equipment are the responsibility of the Security Officer **and** the individual generating and using the data in those systems. The use of a unique identifier for each individual user of stand-alone equipment is recommended, but may be required based on the level of security as identified by the owner of the data.

3. Network Security. Network security is divided into two areas of control: a) wide area networks, and b) local area networks. ChildNet staff is to follow network security procedures which may be designated and updated by MIS Services staff to maintain and enhance network security in accordance with this policy.

a. Wide area networks in this context are controlled by the ChildNet's MIS department. ChildNet may utilize the DMS statewide telecommunication backbone Router Transport Service (RTS) to gain access to state computer systems. Systems such as the Florida On-line Recipient Integrated Data Access System (FLORIDA), Client Information System (CIS), Statewide Automated Child Welfare Information System (SACWIS), etc. utilize the RTS as the primary communications line. Security of the RTS network is the sole responsibility of the DM.

b. Local Area Networks in this context refer to all ChildNet controlled LAN and WAN circuits. Access to ChildNet systems on these networks is allowed.

4. Data Backup

   a. Implement Grandfather, Father, Son (GFS) Backup Strategy for all mission critical network resources (network files, database, and server states).

   b. Implement SQL DB Maintenance Plans on all SQL Database servers to backup databases files and logs to a central repository, which will be included in the GFS backup strategy.

      1. A monthly full backup (Grandfather) will be done on all network resources on the first day of every month

      2. A weekly full backup (Father) will be done on all network resources every Friday

      3. A daily differential backup (Son) will be done on all network resources every day Saturday thru Friday

      4. The full backup is conducted on week-ends, starting on Friday night when activity to network resources are minimal or reduced, to take advantage of a longer maintenance/backup window

      5. A daily differential backup will be conducted every night to take advantage of the faster backup time (compared to a full backup) and a shorter nightly maintenance/backup window. An added benefit of differential backup also is faster restore times (compared to an incremental restore).

Physical / Site Security

1. An annual analysis/review is to be conducted at each location to determine the adequacy of physical/site security. It is to take into account controlled physical

access to the area, the need for disaster contingency planning, and other appropriate security requirements.

2. ChildNet staff is responsible for ensuring appropriate confidentiality and security measures are maintained, and the responsibility of the individual's supervisor to provide adequate training on protection of the information accessed and the physical state of the computer

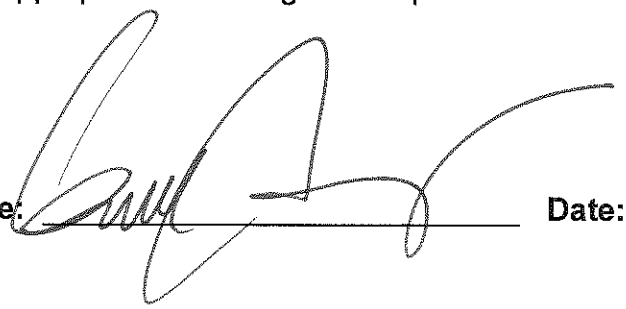
   a. Orientation - ChildNet's Information Security Manager is to be responsible for providing rules, policies, procedures and guidelines on departmental information security which will be made available to and reviewed by all employees during new employee orientation sessions or security awareness training sessions

   b. Training - All new employees review applicable state and federal rules and regulations that pertain to data confidentiality and information security as a part of their pre-service training. Employees are to be advised of the specific security requirements of their positions. Employees are to be notified of any changes to confidentiality laws or changes to ChildNet's security rules, policies, procedures and/or guidelines, or any specific security requirements of their positions by their supervisor and/or Security Officer.

   c. Security Awareness - ChildNet's Data Security Officer is responsible for implementing and maintaining a Security Awareness Training program that is to ensure that employees are aware of the importance of information security. This program is to provide security awareness training to ChildNet staff that utilizes confidential data or automated systems. The Security Awareness Training video is to be presented to all employees and a log is to be maintained by the facilitator of the Security Awareness Training. All employees must attend Security Awareness Training within the quarter after being hired and/or before gaining access to agency systems, or face revocation of their access. Supervisors and security administrators are responsible for ensuring that staff is trained and that appropriate access is allowed.

Audits

The Information Security Manager is to conduct annual internal security audits and evaluations to ensure appropriate users' rights and permissions.

President's Signature:  **Date:** 06-25-14