ChildNet
Leading abused children to safety and stability

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 Federal or state laws, rules, regulations, policies and procedures governing the confidentiality of data are not superseded, abridged, or amended by this operating procedure.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, February 14, 2024
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, is any facility designated by the Information Security Manager that meets specific criteria including, but not limited to, size, infrastructure, security measures, and the criticality of the systems hosted.

Change Advisory Board (CAB) - comprising representatives from MIS, and relevant business units, is established to review and approve significant changes.

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.

Separation of Duties (SoD) - A security principle that divides critical tasks and privileges among multiple individuals or roles to reduce the risk of fraud, errors, and unauthorized access.

Identity and Access Management (IAM) - A framework of policies and technologies ensuring that the right individuals access the appropriate resources at the right times for the right reasons.

User Provisioning - The process of creating, managing, and disabling user access to system and network resources.

Access Review and Certification - Regular audits conducted to assess and confirm the appropriateness of users' access rights to ensure they align with job responsibilities and current needs.

System Administration - Individuals or roles responsible for managing and maintaining the operational functionality of computer systems.

System Engineer - A System Engineer plays a pivotal role in safeguarding an organization's information systems by designing secure architectures and integrating robust security measures to protect against potential threats.

Password Management - The process of creating, storing, managing, and resetting passwords to ensure secure authentication of users.

Audit and Monitoring - Activities undertaken to review and analyze access controls, user activities, and system configurations to ensure adherence to security policies and identify potential security issues.

Change Management - A systematic approach to managing all changes made to a system's configuration and its applications to ensure that no unauthorized changes are made and all changes are documented.

Release Management - The process of managing, planning, scheduling, and controlling a software build through different stages and environments, including testing and deploying software releases.

Incident Response - An organized approach to addressing and managing the aftermath of a security breach or cyberattack, with the aim of limiting damage and reducing recovery time and costs.

Multi-factor Authentication (MFA) - A security system that requires more than one form of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Single Sign-On (SSO) - An authentication scheme that allows a user to log in with a single ID and password to access multiple related, yet independent, software systems.

Continuous Monitoring - The ongoing process of detecting, reporting, and responding to security threats by continuously observing activities and behaviors across the organization's networks and systems.

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. **Systems and 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.

   c. **ChildNet's firewall** is a critical component of its network security framework, designed to regulate incoming and outgoing network traffic based on an established set of security rules. This process aims to protect the organization's network infrastructure from unauthorized access, cyber threats, and malicious activities.

The firewall policy includes:

a. **Rule Definition**: Clear, concise rules are established to control traffic based on source, destination, and type of traffic. These rules are designed to minimize openings in the network and are regularly reviewed and updated to adapt to new security threats.

b. **Default Deny**: All inbound and outbound traffic not explicitly allowed by the firewall rules is denied by default, ensuring that only known and approved traffic can traverse the network.

c. **Segmentation:** The network is segmented into different zones (e.g., public, private, DMZ) with specific firewall policies applied to each segment to control access and limit the potential spread of threats.

d. **Logging and Monitoring**: All traffic passing through the firewall is logged, and these logs are actively monitored for suspicious activities. This enables timely detection and response to potential security incidents.

e. **Regular Updates and Maintenance:** The firewall firmware and software are kept up to date with the latest security patches and updates to protect against known vulnerabilities.

f. **Testing and Audits:** The firewall configurations and policies are regularly tested and audited to ensure they effectively protect against current threats while not impeding legitimate network traffic.

4. Data Transmission

To ensure the privacy and security of data transmitted between providers and the ChildNet application, all in-transit communication is encrypted current industry best practices for secure data transmission, as approved by ITO. All data point access to the ChildNet environment are transmitted over secure channels, as VPN, TLS and SFTP.

5. Encryption

All PII data is stored using strong encryption methods as per current industry best practices, subject to approval by the ITO. Additionally, disk encryption with robust algorithms safeguards all workstations, securing sensitive data against unauthorized disclosure and theft.

6. Remote Access

a. Only authorized persons may remotely access the ChildNet's network. Remote access is provided to those employees, contractors, and business partners of the ChildNet that have a legitimate business need to access internal resources. Remote users' network access is restricted according to their role and as required to fulfill the duties of their jobs.

b. Remote access to the ChildNet network requires a VPN connection, secured, and encrypted using IPSEC/TLS protocols. VPN authentication requires a valid account ID and credentials as well as a host-based certificate issued to authorized devices only as a second authentication factor. Only authorized devices may connect to the ChildNet's network, this includes any company-issued devices that comply with the security guidelines of the ChildNet.

7. System Patching and Vulnerability Scans

a. Continuous vulnerability scans in production and sensitive areas to detect potential security breaches.

b. Critical and High severity vulnerability and security patches must be remediated or mitigated as soon as possible and within 14 days of discovery. Lower risk findings will be addressed in a reasonable and timely manner. Newly discovered vulnerabilities and zero-days are assessed by the Security teams to estimate their potential effect on the environment and overall security posture and mitigated accordingly.

c. Monthly updates for workstations and software, tailored to usage and vendor support, with a comprehensive vulnerability management process.

d. Before deploying to production, a testing environment that mirrors the production setup is essential for thorough evaluation. This environment allows for testing updates in conditions similar to live operations, ensuring updates are compatible with existing systems, minimizing service disruptions, and verifying the effectiveness of new security measures.

e. Operational systems must use software that is actively supported by the vendor. This includes regular updates and patches provided by the software supplier to ensure that all systems are protected against known vulnerabilities.

8. Baseline Configuration and security configurations

a. **Baseline Configuration Management:** Employ configuration management tools to automate the deployment, operation, and enforcement of baseline configurations across all systems.

b. **Web Browser Security**: To leverage the latest security functions and protections against web-based threats, all operational systems within ChildNet must use the latest versions of web browsers. The MIS department shall enforce a policy for regular updates of web browsers to ensure compatibility with the latest security standards and functionalities. This will include monitoring for new browser releases and coordinating the deployment of updates across the organization.

c. **Security Parameter Configuration:** System security parameters are meticulously configured to minimize vulnerabilities and prevent misuse. This includes setting access controls, password policies, and encryption standards to safeguard data integrity and confidentiality.

d. **Supporting Technical Controls:** All operating systems and critical infrastructure within ChildNet must employ a set of supporting technical controls to enhance security. This includes, but is not limited to, antivirus software, file integrity monitoring systems, port filtering tools, and comprehensive logging capabilities. These controls are to be configured according to industry best practices and ChildNet's internal security standards to ensure the confidentiality, integrity, and availability of data and systems.

e. **Continuous Monitoring and Compliance:** Continuous monitoring mechanisms are in place to ensure ongoing adherence to baseline configurations and the effectiveness of security parameter settings. Automated compliance tools assess systems against the baseline to identify unauthorized changes or misconfigurations. Non-compliance issues should be addressed promptly to mitigate potential security risks.

f. **Change Control:** A formal change control process is established for managing alterations to the system configurations. All changes are documented, reviewed, and approved by designated authorities to ensure they do not compromise system security or deviate from the baseline configuration.

g. **Pre-Production Testing:** Before any application or operating system is deployed into the production environment, it must undergo rigorous testing for usability, security, and potential impact on existing systems and data. This testing should include, but not be limited to, security vulnerability assessments, usability testing, and compatibility checks with existing infrastructure.

9. Change Management

a. All changes must be documented in a change management system, detailing the purpose, scope, impact, implementation plan, rollback plan, and security considerations.

b. The impact of the proposed change on system security, data integrity, and operational continuity must be assessed. This includes evaluating potential vulnerabilities, compliance implications, and the need for stakeholder communication.

c. Minor changes may be approved by direct supervisors or system owners. Significant changes require CAB review and approval.

d. Emergency changes, while expedited, must be retrospectively reviewed by the CAB.

e. Changes must be tested in a non-production environment to validate functionality and assess unforeseen impacts. Security-specific testing, such as vulnerability scanning should be included as necessary.

f. Changes are to be scheduled during maintenance windows, minimizing operational disruption. All employees must be notified in advance.

g. Post-implementation, changes must be reviewed to ensure objectives were met and no unintended consequences occurred.

h. All changes must be documented in a central repository with details including purpose, scope, impact analysis, implementation plan, rollback plan, and security considerations. Each change must include a clear rollback plan to revert the system to its previous state in case of failure or unexpected impact.

10. **Access Control Procedures** - ChildNet adheres to the principles outlined in Data Classification And Access Control (CFOP-50-27) ChildNet's access control procedures are designed to enforce these principles by;

a. Access requests will be presented to the Information Owner, or their designated staff, using the appropriate Access Request form or electronic form.

b. Special needs for other access privileges will be dealt with by the Information Owner on a request-by-request basis.

c. The list of individuals with access to confidential or restricted data must be reviewed for accuracy by the relevant Information Owner, or their designated staff, in accordance with a system review schedule consistent and compliant with state and federal laws. The system review schedule must be approved by the Information Owner.

d. **Need To Know:** Each of the requirements set forth in this operating procedure are based on the concept of need to know and the principal of least privilege. If an ChildNet employee is unclear how the requirements set forth in this operating procedure should be applied to any particular circumstance, he or she must conservatively apply the need-to-know concept and confer with their supervisor for guidance. Information must be disclosed only to those employees who have a legitimate business need for the information.

e. **System Access Controls**: The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on any ChildNet business system.

f. Data used for authentication shall be protected from unauthorized access.

g. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to ChildNet systems and their resources.

h. **Termination of Access**: Upon an individual's termination or separation from ChildNet, HR is to request removal of previous authorized system access within 24 hours of determining system access is no longer appropriate, including any Administrative Accounts.

1. Notification ticket should include the name of each IT resource the employee had access to and the date and time of the access. This includes deactivating user accounts, securing or erasing authentication credentials, and ensuring the return of all ChildNet assets.

2. When a ChildNet employee changes from one position description to another within ChildNet, it is the responsibility of the HR department to notify the MIS department about this change. Subsequently, it becomes the responsibility of the MIS department, in coordination with the employee's new supervisor, to oversee the removal of unnecessary access to IT resources. The removal process should be documented in the help desk ticket request.

11. **Identity and Access Management (IAM):** ChildNet commits to rigorous IAM compliance, ensuring all applications and systems adhere to:

a. Multi-factor Authentication (MFA): Mandatory across all platforms, enhancing security by requiring multiple verification forms before granting access.

b. Single Sign-On (SSO): Implemented to streamline user access across various applications while maintaining the capability for thorough monitoring and auditing.

c. Continuous Monitoring: Ensures real-time oversight over user activities, with robust logging mechanisms to support detailed security analyses and audits.

d. Access rights shall be reviewed at least quarterly and immediately adjusted in the event of role changes or terminations, ensuring alignment with current job responsibilities. The process for these adjustments will be documented and overseen by the Information Security Manager

e. **Separation of Duties (SoD):** Integrating SoD within ChildNet's IAM processes is crucial to prevent excessive control or authority concentrated in a single individual's hands, significantly reducing fraud, errors, and unauthorized access risks.

   1. **User Provisioning and Approval:** Access provisioning is segmented into distinct phases where the request for access by a user's manager or supervisor is independently reviewed and approved by a different authority, such as an MIS administrator or an HR personal.

   2. **Access Review and Certification:** Regular audits conducted by personnel not involved in the initial user provisioning, like direct supervisors, ensure that access privileges are continually aligned with the user's current job responsibilities.

   3. **Helpdesk and System Administrator:** Clear delineation of roles is maintained where helpdesk focus on operational aspects, and system engineer and ITO are responsible for overseeing access controls and security policies, ensuring no overlap that could lead to unauthorized access or changes.

12. **Data Classification Procedures-** ChildNet's data classification framework is guided by the standards set forth in DCF Data Classification And Access Control (CFOP-50-27), categorizing data into restricted, confidential and public to protect sensitive information and ensure compliance with state regulations.

    a. All electronic information owned by ChildNet and managed by ChildNet must have a designated Information Owner.

    b. Production information is information routinely used to accomplish business objectives. Owners should be at the level of Director or above.

    c. Information Owners are responsible for assigning one of the three appropriate sensitivity classifications as defined below. Information Owners do not legally own the information entrusted to their care, instead they are designated members of the ChildNet's management team who act as stewards, supervising the ways in which certain types of information are used and protected.

       1. **Restricted (Level 1).** This classification applies to the most sensitive business information that is intended for use strictly within ChildNet . Its unauthorized disclosure could seriously and adversely impact ChildNet, its providers, family, its business partners, and its vendors.

       2. **Confidential (Level 2).** This classification applies to less-sensitive business information that is intended for use within ChildNet. Its unauthorized disclosure

could adversely impact ChildNet or its customers, vendors, business partners, or employees.

3. **Public (Level 3).** This classification applies to information that has been approved by ChildNet's management for release to the public. By definition, there is no such thing as unauthorized disclosure of this type of information, and it may be disseminated via ChildNet without potential harm.

d. Owners and Access Decisions. Information Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. ChildNet take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

13. Data Backup and Disaster Recovery Strategy

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).

c. **Offsite Backup Implementation**: Critical data is duplicated to a geographically distant facility, safeguarding against localized incidents. This approach ensures operational continuity under adverse conditions.

d. **Quarterly Backup Testing Protocol:** Involves systematic verification of data recoverability from both onsite and offsite backups, assessing restoration speed and data integrity, to guarantee reliability in disaster scenarios.

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 IT Officer.

   c. **Security Awareness**

      1. 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 all ChildNet staff.

      2. The Security Awareness Training 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 ten (10) days of hire or face revocation of their access.

      3. Supervisors and security administrators are responsible for ensuring that staff is trained, and that appropriate access is allowed.

4. Employees must pass a security test, based on ChildNet's security policy to have access to ChildNet's systems. Email phishing simulations to all employees are conducted twice a year, to raise awareness against email-related risks.

5. To ensure that security awareness remains current and effective, an annual refresher training is also mandatory for all employees. This yearly training is designed to update the staff on evolving security threats, new policies, and best practices in information security.

Operational Controls

1. Monitoring and Logging

a. ChildNet uses a set of monitoring tools to monitor its services, network devices, and servers. Alerts are sent to relevant MIS staff by email, based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency. The production environment, including the servers and application, is monitored 24/7/365 by a suite of monitoring tools. Key ChildNet staff members are notified of events related to the security, availability, or confidentiality of service, based on pre-defined rules.

b. Systems are in place to log network security events. Logs are retained and monitored in a centralized log collection and alerting SIEM system. The SIEM system configured to send alert notifications to the Information Security team when predefined thresholds are exceeded, or malicious activity is detected.

c. All system activities involving the creation, reading, updating, and deletion (CRUD) of covered information must be logged. This includes user access events, data manipulation, and system changes.

d. Service interruptions, maintenance and updates are communicated to staff through email, or via dedicated communication tools.

e. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Some of these monitoring activities include external audits, internal audits, security testing, misconfiguration scanning, measurements and metrics, vulnerability management and controls audits as part of risk assessment.

2. Compliance Update

a. This policy will be reviewed annually and updated as necessary to remain compliant with federal and state laws and regulations. The Information Security Manager is responsible for initiating this review.

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