ChildNet

Leading abused children to safety and stability

Policy: Password Policy

ChildNet Number: CN 012.019
Original Approved Date: June 22, 2010
Policy Revised Date(s):
Policy Sunset Date:
COA Standard(s): FIN 2, RPM 6.01

Statement of Policy:

ChildNet's policy is to ensure that appropriate secure password protocols and measures are implemented and followed to protect the viability and integrity of ChildNet's computer and communications networks and resources.

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

Procedure: Password Policy

ChildNet Number: CN 012.019
Original Approved Date: June 22, 2010
Procedure Revised Date(s): September 11, 2013, June 10, 2014, February 14, 2024
Procedure Sunset Date:
COA Standard(s): FIN 2, RPM 6.01

Definitions (If any)

Statement of Procedure

This policy encompasses all ChildNet employees, contractors, and vendors with access to ChildNet's systems who require passwords to access local internet/intranet resources and network systems. In establishing these password management and access control standards, ChildNet adheres to the guidelines and best practices as outlined in Security Data and Information Technology Resources (CFOP 50-02) and NIST 800-53, ensuring that all personnel are granted access in a manner that is secure, compliant, and consistent with state-mandated protocols for information security.

Access to the ChildNet Network

A valid user ID and password are required to access the ChildNet office network. New or modified user access to the network is assigned by the MIS team. Administrative access to the ChildNet network is restricted to authorized personnel only and password security parameters have been configured on the network as follows:

Password Complexity:

- Standard Accounts: At least 12
- Privileged Accounts: At least 16 characters

Password Change Interval:

- Password changes is determined by the associated risk level of the account or system. Standard accounts may extend password changes up to 180 days, while privileged accounts should consider a more frequent change schedule, not exceeding 90 days, depending on the risk assessment outcomes.

Account Lockout Mechanism:

- After 5 consecutive unsuccessful login attempts, accounts will be temporarily locked for a minimum of 15 minutes, mitigating brute force attack risks.

Secure Password Storage and Encryption:

- Passwords must be stored using strong encryption standards. ChildNet endorses the use of reputable password managers for secure password storage and management.

Password Confidentiality:

- Passwords are personal and must not be shared. For tasks requiring shared access, utilize role-based access control (RBAC).

Secure Password Recovery:

- Password recovery processes will be secure, requiring identity verification to prevent unauthorized access.

Broader Security Framework Integration:

- This policy is part of a comprehensive security strategy, encompassing:
  - **Mandatory MFA**: Required for all accounts, enhancing security beyond traditional passwords.
  - **SSO Capabilities**: To streamline access while maintaining security and auditability.
  - **Continuous Monitoring and Auditing**: Ensuring visibility over access patterns and potential security threats.
  - **SoD Principles**: Preventing concentration of access that could lead to security risks.

Compliance and Enforcement:

- Regular audits will verify compliance, with necessary adjustments based on findings.

Education and Training:

- Comprehensive training will be provided to all users, highlighting secure password practices and the importance of adherence to this policy.

Access to file shares, application modules, databases, and other computing resources is limited to personnel with direct job responsibilities. Access to information and IT system resources will be granted on a need-to-know or 'minimum required' basis and must be authorized by a combination of the immediate information owner or ITO (Information Technology Officer). Only authorized users have the ability to access Personally Identifiable Information.

See also CN 012.017 Virus Prevention and CN 012.003 Electronic Mail.

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