CHILDREN'S NETWORK OF SOUTHWEST FLORIDA

Policy and Procedures

DEPARTMENT NAME Information Technology		
SUBJECT Password Policy		**POLICY NUMBER:** IT- 004
APPROVAL:	**Effective Date:** 6-19-2017	**REPLACES :** New policy

I. **PURPOSE:** The CNSWFL IT Password Policy is an important aspect of assuring the security and protection of CNSWFL information systems, data, and client records.

II. **REVIEW HISTORY:** New policy.

III. **CONTACT:** Chief Financial Officer

IV. **PERSONS AFFECTED:** All employees of the Children's Network and anyone who has access to electronic equipment of the Children's Network.

V. **POLICY:** All Children's Network of Southwest Florida, LLC technology systems are required to be secured by password and this policy meets or exceeds regulatory requirements such as HIPAA (45 CFR § 164.308), FISMA (44 USC § 3541), GLB (15 USC § 94), and other applicable state and federal regulations.

VI. **RATIONALE:** It is the responsibility of the employees assigned and/or provided with access to CNSWFL systems to take appropriate steps as stated in this policy in the selection and handing of passwords.

VII. **CROSS REFERENCES:** HIPAA, Department of Children and Families CFOP 50-22.

VIII. **DEFINITIONS:**

A. Internet: A global system of interconnected computer networks that are linked together by a broad array of electronic, wireless and optical networking technologies and carrying a vast array of information resources and services such as hypertext documents: the World Wide Web and the infrastructure to support electronic mail.

B. Information Technology Resources: Data processing hardware (including desktop computers, laptops, tablets, smartphones and associated devices),

software and services, supplies, personnel, facility resources, maintenance, training or other related resources.

C. Privately Owned Devices: Information technology resources that are not the property of the Children's Network.

IX. PROCEDURES:

A. Relevant Controls

1. The CNSWFL IT Department and our help desk services in order to assure successful management and to establish a secure information technology environment adhere to the COBIT Governance and Control Objectives established by the Information Systems Audit and Control Association (ISACA®). The following are the relevant controls applicable to our password policy:

2. DS5.2b - A security awareness program is in place and should communicate the security policies to users and include, at a minimum: Password management practices (e.g., selecting/changing passwords); Physical access controls (e.g., use of access cards, escorting visitors); Incident reporting/investigation process; Information storage; Distribution of information; Disposal practices

3. DS5.3b - Password policies and procedures are in place to restrict unauthorized access: Password aging (maximum 90 days); Minimum password length of 6 characters; Password complexity enabled (alphanumeric); Password history of > 3; Enable account lockout (max attempts).

B. Password Standards

1. Employees must change all user-level passwords (e.g., email, web, or computer) at least every 90 days.

2. The minimum password length is 8 characters for all financially significant systems (e.g., Financial Edge, Razors Edge).

3. Passwords must be alphanumeric.

4. Employees must select a password that is different from their 3 previous passwords for a particular system.

5. Employees will be locked out of the system after 3 unsuccessful login attempts. If locked out, Employees must contact the CNSWFL IT Help Desk to reset the password.

6. Employee accounts that have system-level privileges granted through group memberships or programs, such as "Domain Admins," must have a unique password from all other accounts held by that employee.

7. Employees must not insert passwords into email messages or other forms of electronic communication.

8. Employees must not share passwords with anyone in person, in email, or over the phone, including administrative assistants, secretaries, bosses, coworkers, or family members. If someone demands a password, employees should refer them to contact the IT Director.

9. If an account or password is suspected to have been compromised, employees must report the incident to the CNSWFL IT Help Desk and change all existing passwords.

10. If the CNSWFL IT Help Desk suspects the account may have been compromised, such as in the case of seeing an account being used on multiple devices at the same time, the account many be temporally suspended until it can be verified by the employee and/or their supervisor.

C. Password Guidelines

1. Strong passwords are crucial to the security of data at CNSWFL. As such, all employees should know how to select strong passwords and should employ these passwords for all systems to which they have access. The following are characteristics of strong passwords:

a. Contain both upper and lower case characters (e.g., a-z, A-Z).

b. Contain special characters (e.g., !@#&*()_+~-=\<>?,./), letters, and numbers.

c. Are at least eight (8) alphanumeric characters in length.

d. Do not contain a word in any language, slang, etc.

e. Are not based on personal information, names of family, etc.

2. Employees should try to create passwords that are easy to remember but hard for someone else to guess. One way to do this is create a password based on a title, affirmation, or other phrase. For example, the phrase might be "This May Be One Way To Remember," and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

3. Employees should avoid the following when selecting passwords:

a) Names of family, pets, friends, co-workers, fantasy characters, etc.

b) Computer terms and names, commands, sites, companies, hardware, software.

c) The words "CNSWFL" or any derivation of the company name.

d) Birthdays and other personal information such as addresses and phone numbers.

e) Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.

f) Any of the above spelled backwards

g) Any of the above preceded or followed by a single digit (e.g., secret1, 1secret).

D. Password Protection Guidelines

Passwords should be considered sensitive, confidential company information. To protect password(s), employees should adhere to the following guidelines:

1. Employees should not use the same password for CNSWFL accounts as for other non-CNSWFL access (e.g., personal email account, bank PIN number). Where possible, employees should not use the same password for different CNSWFL access needs. For example, your CNSWFL network account password should not be the same used on ASK, FSFN, or Financial Edge.

2. Employees should not write passwords on questionnaires, security forms, or papers stored anywhere in the office. Also, employees should not store passwords in a file on any computer system (including smartphones, or similar devices) unless the device is encrypted and password/lock protected.

3. Employees should not attach their password(s) or device encryption password(s) on the device, keyboard, under the keyboard, or written down and stored with the device especially if the device is a laptop and/or contains client or protected medical information.

4. Employees should not use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook).

5. The IT department may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the employee will be required to change it.

6. The IT department will remove and securely destroy any password(s) information found attached to any equipment. Those exposed password(s) will be required to be changed and may be assigned by the IT department.

E. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including, but not limited to, termination of employment or regulatory actions.