'SOUTHERN HIGHLANDS COMMUNITY MENTAL HEALTH CENTER

POLICY AND PROCEDURE MANUAL

Date of Issue: 11/8/17 **Section Number 244**
Date Revised:
Date Reviewed: 6/24/20

Policy 244 – Password Policy

I. POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Southern Highlands resources. All users, including contractors and vendors with access to Southern Highlands systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All passwords are to be treated as sensitive, confidential Southern Highlands information. This policy applies to any electronic devises requiring credentials to be used for work purposes, such as: desktops, thin clients, laptops, cell phones, etc.

II. PURPOSE

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, and frequency of password changes.

III. PROCEDURE

A. Basic Protection of Passwords

The password must be unique to individual employee. The password must not be shared or given to managers, co-workers, or IT staff. This will prevent multiple users from sharing one computer account and will reduce the risk of a security breach, as well as making it easier to investigate security concerns.

If a password is shared, all employees who are involved in the incident will be liable for any damages, and the infraction may result in disciplinary action.

Work provided cell phones or personal cell phones which are used for work purposes and linked to Windows Outlook must have password protection enabled. Without the use of password protection on such devises, the IT Department may erase/wipe the mobile devise to protect data breach regarding Southern Highlands information.

B. Physical Security of Passwords

Passwords should not be written down. If written down, the physical copy of the password must be locked in secure location, such as a lockable file cabinet, case, or desk drawer. The password must not be placed in visible sight; this includes

posting the password on the computer monitor or under the keyboard. Passwords shall not be sent via unencrypted email. Users must log off before leaving a computer unattended. Offices should be locked to prevent physical security threats or individuals entering your office without permission. Even though the computer may be left for a short period of time, the computer must be locked by navigating to lock the computer (shortcut: press Windows Key and L key, or press the Ctrl+Alt+Del keys and select Lock Computer).

C. Security Concerns

Report any suspicion of your password being stolen or used immediately. If anyone is asking for your password, contact the IT Department. There is no acceptable reason to share your password with any Southern Highlands employee or non-employee.

If any employee needs assistance with using password protection on cell phones, or any other questions regarding the password policy, please contact the IT Department.

IV. STRONG PASSWORD REQUIREMENTS

A. Complexity

1. Passwords must be at least eight characters long with uppercase, lowercase and a number, and must be changed every 90 days.

2. Passwords cannot contain the user name or parts of the user's full name, such as the first name.

3. Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

B. History

Enforce Password History – This sets how frequently old passwords can be reused. Users may not reuse any of the last four passwords.

Maximum Password Age – This determines how long users can keep a password before it must be changed. Passwords must be changed at least once every 90 days.

Minimum Password Age – This determines how long users must keep a password before it can be changed. Passwords cannot be changed more than one in a 30 day period.

C. Lockout and Reset

Multiple failed attempts, in a short period of time, to log into the system will result in the account being temporarily locked as a security feature. This will prevent unauthorized users from gaining access to Southern Highlands data. When this occurs, the employee can contact the IT Department to reset their password to a temporary password and re-enter the account. The user must then create a new password to replace the temporary password upon logging in to the system.

Invalid attempts and account lockout – Accounts with five consecutive incorrect attempts will be locked.

Account Lockout duration – Accounts which have been locked due to multiple failed login attempts will remain locked until reset by the IT Department.

V. SYSTEM ADMINISTRATIORS RESPONSIBILITIES

A. At initial login, each user will be given a temporary password. The user will be prompted to change the password at the first login.

B. System administrators must configure a user to require a password before allowing the user access to the system.

C. System administrators shall not use default passwords for administrative accounts.

D. System administrators must utilize system configurations to lock an account after excessive consecutive failed login attempts, suspicious password activities, and any other perceived security concern.

E. Successful and failed login attempts must be tracked.

F. Compromised account passwords must be reset or the account must be disabled to combat the threat of security breach.

G. System administrators must periodically audit the use of passwords and ensure that system configurations are working properly to ensure for continued protection of sensitive data.

VI. DELCARATION

Any devise that does not meet the above security requirements outlined in this policy may be removed from the Southern Highlands network until the devise can comply with this policy.

ENFORCEMENT

All officers, agents, and employees of southern Highlands Community Mental Health Center **must** adhere to the Password Policy, and all supervisors are responsible for enforcing this policy. Southern Highlands CMHC will not tolerate violations of this policy. Violation of this policy is ground for disciplinary action, up to and including termination or employment and criminal or professional sanctions in accordance with Southern Highlands CMHC's medical information sanction policy and personnel rules and regulations.

I have read, understand and acknowledge receipt of the Password Policy. I will comply with the guidelines set out in this policy and understand that failure to do so may result in disciplinary action up to and including termination of employment.

Signature: _____

Date: _____

Printed Name: _____