Effective Date: 7/1/2019
Review Date: 9/26/2023
Revised Date: 7/6/2023

North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Access Codes and Passwords

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 9/26/2023 Signature:

POLICY #4002.00

SUBJECT: ACCESS CODES AND PASSWORDS

POLICY

North Sound Behavioral Health Administrative Services Organization's (North Sound BH-ASO) mission and guiding ethical principles place great value on the privacy and confidentiality of information. Beyond these principles, privacy and security are mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2. These regulations require that North Sound BH-ASO deploy and maintain a policies, procedures, best practices, and other technologies to safeguard confidential information and ensure information is not disclosed to anyone without the proper authorization to view or possess such information.

Access Codes and Passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. Passwords used to log into any confidential system, network or web application are considered Category 3 data and must be protected as such.

The IT department will institute a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use North Sound BH-ASO computer systems and network. The characteristics of the password requirement consist of the following:

1. The password must consist of at least 10 alphanumeric characters from at least three of the following:
    a. Upper case letters
    b. Lower case letters
    c. Numbers
    d. Special characters (*, #, &, etc.)
2. Each user must change their password every 90 days.

IT Department Responsibilities

1. The IT department shall be responsible for the administration of access controls to all company computer systems.
2. The IT department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.

3. The IT department will maintain a list of administrative access codes and passwords and keep this list in a secure area.
4. Set the default to change passwords at least every 90 days.
5. Set the default so that service account passwords must consist of at least 20 alphanumeric characters if the system supports it and include at least three of the following: Upper case; Lower case; Numbers; Special Characters.
6. Set the default to activate a password protected screensaver, set for 10 minutes.
7. Set the default that after three failed attempts to log on, the system will refuse to permit access for 30 minutes. Cell phones will lock the device after 10 failed login attempts. Administrator intervention will be required to restore access to the device once it has been locked out.
8. Set the default for a password history of 24 remembered passwords.
9. No less than annually, the IT department will conduct an audit of the access code and password policy and practice.

Employee Responsibilities
Each employee:

1. Shall be responsible for all computer transactions that are made with their User ID and password.
2. Shall not disclose passwords to others. This should be strictly interpreted by all staff.
3. Passwords must be changed immediately if it is suspected that they may have become known to others. If an employee suspects or knows that their password has become known to another person, the employee should immediately report this event to the IT Department.
4. Passwords should not be recorded. This means that passwords should not be written on "sticky" notes on the monitor, placed on paper, taped to the bottom of the keyboard, etc.
5. Will change passwords at least every 90 days.
6. Should use passwords that will not be easily guessed by others, and do not contain dictionary words.
7. Should log off or lock their desktop workstation when leaving the ASO office.
8. Should log off or lock their home office laptop when leaving it unattended.

Emergency Access to Applications/Files
An emergency may arise in which a user needs access to a system resource that is password-protected under another user ID and where that user is unavailable. In no circumstance should the original user ID account owner's password be shared to access the application/files. To have a clear chain of responsibility, IT support will make available the application/file as needed and is able.

Managers' Responsibility
Managers should notify the IT department promptly whenever an employee has provided notification that they are intending on leaving the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Enforcement
All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with North Sound BH-ASO's Employee Conduct and Discipline policy.

ATTACHMENTS
None