Utah Department of
Health & Human Services
Services for People with Disabilities

PASSWORD PROTOCOLS FOR NATIONAL CORE INDICATORS (NCI) ODESSA SOFTWARE

Directive 1.55

Authorizing Code: 62A-5-103
Rule: NA
Version Date: September 2022
Next Review: September 2024

Forms: NA

Purpose

This policy is to establish password and access protocols for users of the National Core Indicators (NCI) Online Data Entry Survey Application (ODESSA) software platform.

Definitions

ADMINISTRATOR - means a role within the ODESSA software system assigned to certain DSPD staff.

DHHS - means the Utah State Department of Health and Human Services

DIVISION (DSPD) - means Division of Services for People with Disabilities, within DHHS.

NCI - means National Core Indicators.

ODESSA - means NCI's Online Data Entry Survey Application software application.

OSR - means Office of Service Review, a unit within the DHHS Division of Continuous Quality Improvement (CQI).

SCE - means a contracted service coordination provider.

Policy

1. Roles and Access Levels:
    a. Assigned staff from the Division of Services for People with Disabilities (DSPD) will hold administrator-level rights within the system.
    b. DHHS staff will hold user-level rights in order to enter survey responses.
    c. Contracted SCEs will hold user-level rights in order to enter the demographic/background section of the survey.

2. Password and Account Access:
    a. Administrators will require OSR users to create a new password every 90 days.
    b. When resetting passwords for OSR users, the administrator will notify the user that they must create a new password that adheres to the password requirements listed below in section 3.
    c. Administrators will terminate SCE user access accounts six weeks after creation.
    d. When restoring SCE accounts annually, the administrator will instruct the SCE user that they must create a new password that adheres to the password requirements listed below in section 3.
    e. All administrator-level passwords must be changed every 60 days;
    f. Whenever someone with access to administrator-level passwords leaves employment with DHHS, their account will be terminated.
    g. All user-level passwords must be changed at least every 90 days.

3. Strong Password Requirements - passwords must meet the following requirements:
    a. Passwords must be <u>at least eight characters in length</u>.
    b. Passwords may not include any portion of a user's name, address, date of birth, Social Security Number, username, nickname, family name, pet name, sports team name, or any word that appears in a dictionary, or any such word spelled backward.
    c. Passwords must include at least one character from among three of the following attributes:
        i. uppercase characters (A – Z)
        ii. lowercase characters (a – z)
        iii. numeric characters (0 – 9)
        iv. special characters (i.e. !, @, #, $, %, ^, &, *,))
    d. A user may not reuse any previously used password.
    e. A user may not simply add a number to the end of a previously used password.