UTAH DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF SERVICES FOR PEOPLE WITH DISABILITIES
POLICY AND PROCEDURES

Policy: 1.55	**Page 1 of 2**

PASSWORD PROTOCOLS FOR NCI ODESA SOFTWARE

RATIONALE:
The intent of this policy is to provide guidelines for division staff to follow when creating a secure password for accessing the National Core Indicators (NCI) Online Data Entry Survey Application (ODESA) software platform.

Authorizing Code: 26B-9-403
Rule: NA
Forms: NA

Original Effective:	**Revision:**	**Next Review Due:**
NA	**12/11/2025**	**12/11/2030**

I. DESCRIPTION

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

II. DEFINITIONS

The following terms are defined for this policy as:

A. **Department:** means the Department of Health and Human Services (DHHS).

B. **Division:** means the Division of Services for People with Disabilities as defined in Section 26B-6-401.

C. **National Core Indicators (NCI):** means the system used to share performance measurement for the National Association of State Directors of Developmental Disabilities Services (NADDDS) member states. NCI tracks progress toward person-centered outcomes in the fields of (1) intellectual and developmental disabilities, and (2) aging and disabilities.

D. **ODESA:** means NCI's Online Data Entry Survey Application software application.

E. **ODESA administrator:** means a role within the ODESA software system assigned to certain division staff.

F. **OSR:** means the Office of Service Review, an operational unit within the Division of Continuous Quality Improvement (CQI).

III. POLICY

A. Roles and access levels:

1. Assigned staff from the division data research team shall hold administrator-level rights within the system.

2. Other department staff shall hold user-level rights in order to enter survey responses.

A. Strong password requirements. Passwords must meet the following requirements.
    1. Passwords must be at least eight characters in length.
    2. 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.
    3. 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; and
        iv. special characters: !, @, #, $, %, ^, &, *,), (, etc.
    4. A user may not reuse any previously used password.
    5. A user may not simply add a number to the end of a previously used password.

B. Password updates and termination:
    1. All administrator-level passwords must be changed every 60 days;
    2. All user-level passwords must be changed at least every 90 days.
    3. Whenever someone with access to administrator-level passwords leaves employment with the department, their account shall be terminated.

IV. **PROCEDURE** - Password and account access:

A. ODESA Administrators shall require OSR users to create a new password at least every 90 days.
    1. If the password is not changed by OSR users after 90 days, the administrator shall disable the old password which will force the OSR user to reset their password.
    2. The OSR user must then use the system's change password feature to update it to a password of their choosing.
    3. The administrator shall notify the user that they must create a new password that adheres to the password requirements listed above.

B. Administrators shall update their own password at least every 60 days by clicking the forgot password option on the log in screen and creating a new password based on the requirement listed above.