



POLICY: Local WIC programs shall follow established procedures for TWIST security processes.

PURPOSE: To ensure security of access to TWIST and confidentiality of WIC participant records. Participant data security is essential to the WIC program.

RELEVANT REGULATIONS: 7 CFR §246.26(d)—Confidentiality of applicant and participant information

OREGON WIC PPM REFERENCES: ◆450—Confidentiality

TWIST TRAINING MANUAL REFERENCES: Chapter 1, Lesson 100—Introduction to TWIST and TWIST Security

APPENDICES: DEFINITIONS:

<i>TWIST</i>	The WIC Information System Tracker. The data system for the Oregon WIC Program.
<i>User</i>	A staff member who has access to the TWIST data system.
<i>Role</i>	A designation in TWIST that defines levels of access (edit, view or no access). Roles are assigned to users.
<i>Add-on role</i>	A specialized role in TWIST that does not stand alone. These roles are granted to specific individuals who already have a role in TWIST but need additional access to a certain area of TWIST in order to perform a specific function.
<i>Unique identifiers</i>	Any data element that can be used to identify a participant (<i>i.e., participant name, address, phone number</i>).

PROCEDURE:

- Confidentiality statement*** 1.0 All WIC staff must sign a confidentiality statement to confirm they have been notified that all participant data must be kept confidential. See ♦450--Confidentiality.
- 1.1 Ensure each staff member signs a confidentiality statement when hired and maintain this documentation on file.
- Security roles in TWIST*** 2.0 Security roles shall be assigned and removed in TWIST with the permission of the Local Coordinator or their designee. Staff should be properly trained in the areas of TWIST for which they have security. For a list of roles and their corresponding access, run report SA130R 'FamilyNet User Role Authorities' from the Security module.
- 2.1 The WIC Coordinator or designee is granted the role 'Set User Security Local'
- 2.2 The role 'Set User Security Local' grants the ability to add/remove users, change TWIST passwords, and assign or remove security roles to users.
- 2.3 A user with the 'Set User Security Local' can also grant add-on roles to staff members.
- 2.4 When a staff member is no longer working in the WIC program, the WIC Coordinator or designee must remove their WIC role(s). If they are no longer working in a program that requires them to use Familynet, their name should also be removed from the "Security" table in TWIST.
- Security of TWIST reports*** 3.0 Participant data must be kept secure:
- 3.1 At employee workstations, staff should "lock" their computer screen if they leave their workstation while they have TWIST open.
- 3.2 All documents and reports that are generated from TWIST must be kept secure (i.e. Verification of Certification (VOC), ineligibility notifications, etc.).
- 3.3 Any document or report that includes a participant's name or any other unique identifier must be kept secure.
- 3.4 Keep documents in a locked drawer or file cabinet, turned face down on a staffed workstation, or in an area where non-WIC staff are not permitted.
- 3.5 See ♦450—Confidentiality for more detailed information on security of participant data. ★

**If you need this in large print or an alternate format,
please call (971) 673-0040.
WIC is an equal opportunity program and employer.**