System Security

I. Local agencies should require each end user to sign an Acceptable Use Policy form or other similar form. (This is commonly required by and coordinated with the County/Health Department IT Department).

II. VISION system access is controlled using the Utah ID Single Sign-On system with dual factor authentication.

III. Staff should monitor the use of the computer system to prevent loss of data due to theft, errors, and misuse.

IV. Security Access Request- WIC directors should fill out the ***User Request Access Form***, available on SharePoint in the "Requests" menu for requesting changes to VISION security access for employees. The form is automatically submitted to the WIC Help Desk for the access to be updated.

a. Form uses include:
    i. New employees,
    ii. Terminating access for former employees,
    iii. Providing access to additional or different clinics,
    iv. Requesting role changes,
    v. When changes to security access have been made and need to be reversed, and
    vi. Authorizing certain employees to make security access decisions in place of the WIC director when needed.

b. A separate form must be completed for each staff person.

c. Very temporary changes to roles and clinics will not be allowed. In these situations, permanent changes allowing greater access should be considered.

d. If the employee must have access to intake, assessment and issuing benefits, the access for all three must be approved by the State WIC Director.
    i. Some staff may be granted security access within VISION by the State WIC Director to complete intake screens, nutrition assessment and issue benefits. Though possible, staff should avoid completing all these functions for the same participant.
    ii. In very small clinics that operate with only one staff member regularly or due to temporary circumstances, staff in a role approved by the State WIC Director may complete all certification functions when necessary.
    iii. The Local Agency WIC Director is responsible to audit the work of employees who have been granted full access (State WIC Director

approved role) in order to prevent clinic fraud. (See Monitoring of Staff to Prevent and Detect Fraud).

V. Users must sign off/log off of VISION when leaving the computer workstation. Each individual staff using the terminal must log in with their own VISION credentials; multiple users cannot utilize the same log in.

VI. Issues and errors with the VISION system and with scanner, signature pad, and card reader hardware should promptly be reported to the WIC Help Desk. Other computer hardware issues should be reported to county/local health department IT departments or State DTS as appropriate for the local agency.

VII. Computer hardware should be kept in a secure environment during clinic hours; portable equipment not in use must be locked in a secure location or have a locking device to avoid theft.

VIII. Clinic staff should never change/alter or tamper with the computer's system calendar. The date and time shown in the Windows system tray of the computer (bottom right corner) must be accurate with the current date and time. Changing the system date in the computer causes serious data issues and errors with VISION. Staff altering the system date to attempt to correct issues may be unintentionally committing fraud. Avoid using this as a calendar to prevent accidental changing of the system date.

IX. VISION should not be downloaded to personally owned computers/devices and should not be used outside of the WIC clinic environment without State Office approval.