CHAPTER 3. STARLINC OPERATIONS OVERVIEW

Security

Purpose To provide the local agency procedures for security of the StarLINC system data and equipment.

Policy WIC staff involved in certification is responsible for the safeguarding of WIC participant information, electronic files, and physical equipment used in the administration of the program.

Authority **CFR 246.4 (a) (12)**

Procedure WIC staff shall follow the measures outlined below regarding physical, network, operating system, and application levels of security. WIC staff shall also review (annually) and follow the "Annual Computer Use Agreement" attachment.

- **Physical**
  - Control physical access to all StarLINC equipment.
  - Report any loss\theft of StarLINC equipment immediately to the State office by phone. Follow-up with a written statement.
  - Report theft to local authorities.

- **Network**
  - Use software or hardware-based firewall on WIC clinic networks.
  - Review any actual or suspected information security breaches to both C-Quest and the State Agency.

- **Operating System**
  - Enable strong password policies.
    - An ideal password is long and has letters, punctuation, symbols, and numbers.
    - Whenever possible, use at least 14 characters or more.
    - The greater the variety of characters in your password, the better.
    - Use the entire keyboard, not just the letters and characters you use or see most often.
  - Limit administrative access to system.
  - Ensure updates to the anti-virus protection are being done when connecting to the internet.
  - Ensure computers are connected to the agency network quarterly to ensure the Anti-Virus program updates are loaded.
  - Do not use StarLINC equipment for personal use.
  - StarLINC equipment shall not be used/accessed by any other entity.

- **Application**
  - Require unique logon for all StarLINC application users.

  - Logons for new staff shall be requested by State staff to C-Quest.
  - Request will only be received by supervisor or program managers.
- Enable strong application password policies.
- Passwords cannot be shared under any circumstances.
- Log off the application when leaving your computer.
- Notify the State Office immediately of any staff leaving employment by the agency so their login can be inactivated.
- Report any virus activity or suspicious equipment behavior immediately to the State office or C-Quest for follow-up.

The State Office shall provide C-Quest with contact information of those staff authorized to request changes to the MIS system.