Computer Workstations

Intended Audience

- All ARIES Users
- Managers and Supervisors

Policy Background

Computer workstations, including laptops, which are used (1) to access ARIES directly or (2) to manage data extracted from ARIES, must be kept secure at all times.

Procedures

Agencies need to consider security when setting up computer workstations. For example,

- Where is the computer workstation located? Workstations should not be located in areas where the public can view the screens such as clinic waiting rooms, meeting rooms, or hallways.

- Can clients or other staff see the computer screen? To the extent possible, computer screens should be fitted with screen guards to minimize the possibility of unauthorized staff or clients viewing data on the screen.

Users should lock their computers when not using them. This can be accomplished in two ways:

- Users should electronically lock their computers when they leave their desk. Users can lock their computers by depressing the "L" and Windows keys simultaneously (or conversely, depressing the Ctrl, Alt and Delete keys simultaneously and then hitting the Enter key).

- The screensaver can also be set up to automatically engage when the computer is inactive for a predefined period of time. Users can set up their screensavers by going to the Microsoft Start button and selecting Settings > Control Panel > Display > Screen Saver.

Users who have digital certificates installed on laptop computers may access ARIES with the following caveats:

- Users cannot access ARIES in public locales such as coffee shops, airports, hotel lobbies, or public libraries.

- Data encryption software must be installed and used on these laptop computers.

Compliance Monitoring

The State Office of AIDS (OA) staff will inspect computer workstations as part of their site visits for OA-funded programs.

Related Policies

- ARIES Policy Notice No. B1 regarding Security Incident Reporting
- ARIES Policy Notice No. B4 regarding Mobile Devices