



WORKSTATION ACCESS AND FACILITY SECURITY POLICY

PURPOSE

To establish a policy that provides guidance for workstation security that includes the types and locations of workstations, the approved functions of those workstations and the measures to be used to protect access to information at those workstations.

SCOPE

This policy applies to all LADD support services, and employees.

POLICY

It is the policy of LADD to have established procedures to ensure the confidentiality and availability of PHI to authorized users.

STANDARDS AND DEFINITIONS

Types of Workstations

Location	Workstation Description and Permissible Uses	Access
Remote Workstation	A workstation at a personal residence consisting of either a desktop or laptop and multi-function device. To be used to carry out job responsibilities and support stakeholders.	Director Department Director Regional Director Office Support Staff
Mobile Workstation	A workstation that can be moved and consists of either a laptop or notebook. To be used to carry out the functions of job responsibilities and support stakeholders.	Director Department Director Regional Director Supervisor
Central Office Workstation	A workstation at designated office space with support staff providing administrative support for stakeholders. These workstations consist of desktops, printers, scanners, fax and copier	Director Department Director Regional Director Supervisor Office Support Staff
Program Workstation	A workstation at a LADD operated location such as a licensed program. The workstation is in space designed as office space and consists of desktops, printer, scanner, fax and copier to be used to carry out the functions of the location and support stakeholders.	Supervisor Manager Assistant Manager
Service Site Workstation-Management	A workstation located at a person supported residence. The workstation may be in a designated office space or may be in an area of the home deemed appropriate by the person. The equipment may include a desktop, printer, scanner, fax and copier to be used to carry out the functions of the location and support stakeholders.	Supervisor Manager Assistant Manager
Service Site Workstation-Staff	A workstation located at a person supported residence. The workstation is in an area of the home deemed appropriate by the person. The equipment may include a desktop and printer to be used by staff for documentation. This may include an I pad or tablet to be used in the community for documentation.	Supervisor Manager Assistance Staff (PCT)

Physical Safeguards – Action taken to prevent unauthorized access to PHI and protect buildings and equipment from natural disasters and unauthorized intrusion. May consist of locks, keys, key fobs, screen protectors, strategic placement of screens, alarm systems,

Technical Safeguards – Technology used to secure against unauthorized access to PHI and protect buildings and equipment from natural disasters and unauthorized intrusion. May consist of individualized User ID, password and secondary authentication, , use of software, prohibitions against use devices in conjunction with LADD IT Asset.

*****The following measures must be implemented where applicable*****

- Workstations will be located in secure areas with locked doors or in locked cabinets with keys available to authorized staff only.
- Use of a HIPAA Visitor Log to maintain a list of people who have been in and out of the locations.
 - Steps employees take to validate a person's identity
 - A requirement that all visitors must sign in, including time of arrival and purpose of visit i.e. repair refrigerator, visit family
 - What employees are to do in the event of unauthorized entry or a visitor is not in an area that coincides with the stated purpose of their visit
 - Visitors includes maintenance and repair workers, deliveries and sales people so that all entry to the facility is noted.
 - Visitors may be escorted to the location that coincides with their stated purpose of visit
- Use of AOD to maintain a schedule of employees who are working at locations.
- Use of Emergency Guidelines to minimize the impact of natural or manmade disasters.
- Asset Users will position computer screens away from traffic areas or common areas accessed by visitors.
- Asset Users will not connect removable storage devices to any workstation, this is prohibited
- Asset Users will not save confidential information on workstations unless it is appropriately secured against theft or loss and consult with the IT Dept. or CCO regarding appropriate steps to secure.
- Confidential information, based on the concept of minimum necessary should be saved in folders with access limited to those individuals authorized to access the information.
- Asset Users must logoff or lock their workstations when not in use.
- When appropriate, Asset Users should use a privacy screen to prevent unauthorized people from viewing information on their workstation screen.
- Asset Users must never install software on LADD IT Asset.
- A user ID and password must be required to use all workstations.
- All special access rooms that contain sensitive equipment or information i.e. workstations, file rooms, offices, fax/copy rooms will be locked with appropriate signage prohibiting unauthorized access.
- All LADD faxes will utilize a standardized, approved organizational fax cover and the original faxed information and cover are maintained when part of the person supported record to guard against altering faxed information.
- All unwanted and confidential documents will either be immediately shredded or placed in a bin that is secured against unauthorized access until the documents can be disposed of.
- The chain of custody for keys to secure areas will be monitored at all times and in the event, keys are lost it will be reported to the immediate Supervisor.
- In the event of an unhappy ex-employee who has made threats against another employee, person supported/family or the facility it will be reported to the immediate Supervisor, Human Resource Director and CCO.
- In the event an outside source has made threats against another employee, person supported/family or the facility it will be reported to the immediate Supervisor, Human Resource Director and CCO.

VIOLATIONS

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including separation from employment and possible legal prosecution.