# INFORMATION ACCESS POLICY

## PURPOSE
To establish a policy that identifies the steps taken to maintain an adequate level of security to protect PHI, LADD data and information systems from unauthorized access.

## SCOPE
This policy applies to all LADD support services, employees and business associates.

## POLICY
It is the policy of LADD to have established procedures to insure only secure, approved access to PHI, data and information systems is allowed; that correct levels of access are monitored and reporting mechanisms are in place so corrective action is taken immediately.

## STANDARDS AND DEFINITIONS
**Level of Access** – Notes the level of access each Asset User is given based on job responsibilities and need to know.

| Remote Desktop Drives | Staff | Assistant Manager | Manager | Supervisor | Support Supervisor (By Dept) | Regional Director | Department Director | Executive Director |
|---|---|---|---|---|---|---|---|---|
| Website Employee Section | X | X | X | X | X | X | X | X |
| All Staff (P) | X | X | X | X | X | X | X | X |
| General (K) | X | X | X | X | X | X | X | X |
| Committee (E) | X | X | X | X | X | X | X | X |
| All Managers (O) | | | X | X | X | X | X | X |
| Manager (R) | | | X | X | X | X | X | X |
| Supervisor (J) | | | | X | | X | X | X |
| Management Coverage (L) | | | X | X | | X | X | X |
| Corporate Quality (I) | | | | X | X | X | X | X |
| Administration (G) | | | | | | X | X | X |
| Human Resources (W) | | | | | X | | X | X |
| Finance (Z) | | | | | X | | X | X |
| Quality Assurance (Y) | | | | | X | | X | X |
| LADD IT (X) | | | | | X | | X | X |
| QI and Training (Q) | | | | | X | | X | X |
| FOI (V) | | | | | | | | X |
| Executive (K) | | | | | | | | X |

| Applications | HR Dept | IT Dept | Compliance Dept | QA Dept | Training Dept | Services Dept |
|---|---|---|---|---|---|---|
| AOD | X | | | | X | X |
| File Hold | X | X | | | | |
| Therap | | X | X | X | | X |

**Asset User** – The LADD employee assigned an IT asset to perform their assigned job. Asset Users must protect and use the asset as intended. In the event of theft, loss or damage to the asset the individual, must immediately report the incident to the IT Dept. or their supervisor. Supervisors are responsible for ensuring Asset Users know their responsibilities and are immediately reporting theft, loss or damage to the asset. In addition, Asset Users must:

- Routinely verify the accuracy of email addresses used to send emails
- Use **ladd secure** to secure all emails that contain PHI and are going outside of the closed LADD remote desktop system to insure proper encryption takes place.
- Will maintain login and password per LADD standards.
- All computers used by Authorized Users that are connected to the LADD Information Technology Network, must continually execute approved Virus-scanning Software per the LADD IT Department.

**Asset User Authentication** – Each Asset User will, at all times utilize their unique user name, password and any additional authentication measures to secure access to all IT assets and verify their identity. User name and password is never to be shared or given out. Asset Users are responsible for all action taken under their sign on. All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. All users must be required to change their passwords at least once every 60 days using the following criteria:

Follow these guidelines when creating a password:

- The password must be 7 to 32 characters long.
- The password must contain a mix of letters, numbers, and/or special characters. Passwords containing only letters or only numbers are not accepted.
- The password is case-sensitive.
- Single quotes, double quotes, ampersands ( ‘ " & ), and spaces are not allowed.
- Successive passwords should not follow a pattern.
- Do not post or share your password or send your password to others by email.

Do not communicate or give user names or passwords to others or allow the use of a user name or password by others at any time. **Email Activities** – Special precaution is to be taken whenever using email. The following guidelines must be followed:

- Always secure PHI by encrypting email using **ladd secure** in the subject line of the email,
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email SPAM).
- Any form of harassment via email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Creating or forwarding Chain email, Phishing, or other scams of any type.
- Solicitation of email for any other email address, other than that of the Authorized User’s own account, with the intent to harass or to collect replies is prohibited.

- Creating or forwarding Chain email, Phishing, or other scams of any type is prohibited.

**Workstation Access Control** – Each IT asset that has the ability to be set with an auto log off, time out after no activity and password enabling will be set by the IT Dept. prior to being put into service. All workstations must utilize the installed access controls. Active workstations are not to be left unattended for extended periods and should be logged off when not in use. Automatic Logoff. If an information system has an automatic logoff capability, then the feature will be enabled to terminate an electronic session after a predetermined time of inactivity.

**Minimum Necessary** – PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose, responsibility or function of the job. Based on the "Need to Know".

**Disclosure Notice** – a notice warning Asset Users they must only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.

## PROCEDURE

1. All employees will be given basic access at the staff level as part of the orientation process.
2. For Management level or higher, after completion of the IT Dept. orientation the IT Director will submit a request for access, via email to NSO following the level of access grid above.
3. If there are requests for additional access the IT Director will contact the CCO for approval of the appropriate access level.
4. The CCO will verify the correct level of access for the employee with their Supervisor or HR Dept. and respond to the IT Dept. email with approval and the level of access to be given.
5. If an employee becomes aware of access levels that are not in line with the minimum necessary, they will notify the CCO immediately. The CCO will in turn work with the IT Director to correct access immediately.
6. The IT Dept. will periodically audit and complete regular maintenance to email addresses and email groups.
7. If an employee is suspended or separated their login access will be discontinued as part of the Separation Notice process.
8. If a member of management is suspended or separated their login access will be discontinued immediately as part of the Discharge Management Checklist.
9. The IT Dept. will periodically audit for correct access levels to PHI, LADD data and information systems.
10. The IT Dept. will maintain website security software per the Technology Plan and periodically audit for unauthorized access.



## VIOLATIONS

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