USER ACCOUNT MANAGEMENT POLICY

1 Purpose and Scope

This policy establishes the requirements for creating, updating, and removing user accounts on all CTI IT Systems.

2 Definitions, Acronyms, Abbreviations

- N/A

3 CTI User Account Management Policy

It is the policy of CTI to provide access to its employees (including contractors and other CTI representatives) in a manner that is consistent and appropriate with their job responsibilities. Access will be granted only to requests that have been properly authorized.

3.1 Assigning and Using User Account Names

Users are assigned their own unique user account and password. User account names must clearly relate to a specific person using the person's actual first name (or initial) and last name when possible.

User accounts are for the exclusive use of the named person. Account and password sharing is not permitted.

3.2 New User Accounts

There must be an approved request before a new user account is created. Account requests are submitted to the IT Service Desk and must include:

- Requestor name
- Request date
- User name
- User position
- Requested account start date
- Requested termination date (if applicable)
- Name of application, database, server, or network service required
- Level of access
- Authorized Approver
- Approval Date

3.3 User Accounts Termination

IT Service Desk will disable a user accounts upon notification of termination, or by the Requested termination date (if applicable). User accounts will be disabled at the Active Directory level immediately upon notification. This locks access to CTI's internal networks. Application-level access will be disabled within five (5) business days from the date of notification.

Failure to disable an account according to this protocol shall be considered a security incident.

3.4 Disabling Inactive User Accounts

Application-level accounts that have been inactive for ninety (90) days or more will be disabled by System Administrators. Account activity analysis is conducted on a quarterly basis.

Disabled user accounts may be reactivated only by following the User Access process.

3.5 Changes to User Accounts

Changes to User accounts must be submitted to the IT Service Desk following the same process as new user accounts.

3.6 Annual User Account Review

Authorized Approvers are required to perform an account review annually. The purpose of this review is to confirm current level of access.

4 Enforcement

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of CTI senior management. Severe, deliberate, or repeated breaches of the policy may be considered grounds for instant dismissal, or in the case of a CTI vendor or agent, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

5 References

- *CTI Security Event and Security Incident Reporting Policy*