**I. Purpose:**

a. The computer network and electronic information processing resources of the CLO and affiliates represent valuable assets that contribute significantly to the achievement of the Company's business objectives.

b. The purpose of this policy is to define the high-level guiding principles for implementing network security and to direct the development of further network security controls (policies, procedures, and standards).

**II. Scope:**

This policy applies to all CLO information and network processing assets including employees, contractors, and other related associations.

**III. Background and Justification:**

The company network and information processing represents core assets essential for daily operation. Therefore, maintaining a stable, reliable computing environment.

**IV. Policy Statement**

To ensure effective network security is a team effort involving the participation and support of every CLO employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**V. Roles and Responsibilities:**

Responsibilities for implementing this policy will be governed by the following general assignments:

1. <u>All Users:</u>
   a. This defines all individuals with access to company information and information assets as described in the policy scope. Responsibilities include the following:

   b. Maintaining awareness and complying with relevant company policy, procedures and standards.
   c. Remaining alert for and reporting policy violations to line management or other appropriate contacts.
   d. Taking appropriate measures to safeguard company and client confidential information wherever it is located (e.g. physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.).

2. <u>User Access: (</u>New, Change, Disable, Delete)

   All requests for access should be formally documented via email . Microsoft Outlook will be used to process changes to Administrative privileges on existing servers and the active directory domain. When servers are initially constructed and added to the environment local administrator access is set per the server build requirements which will be included with the Request for Change (RFC) email in the Change policy.

3. <u>User Access Review:</u>

   User access privileges will be reviewed on a monthly and annual basis.

**VI. <u>Data Classification:</u>**

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk.

1. Windows Domain Password Controls:

   The following password parameters will be enforced on all Windows Domain user accounts:

| Domain Password Policy | Security Setting |
|---|---|
| Min. Password Length | 8 characters(includes 1 cap,One num,and One special char) |
| Max. Password Age | 90 Days |
| Min. Password Age | 0 Days |
| Lockout Threshold | 3 |
| Lockout Duration | 5 minutes or unlocked by a System Administrator |
| Min. Password History | 13 |

2. Unique IDs:
   a. All Employee users will be issued unique active directory IDs. Users are not to share credentials at any time with other employees or people outside of the company.

   b. Guests requiring internet only access will utilize the Oklahoma Open wireless access points located across 8th or 9th floor.

   c. Technology Vendors will be assigned a unique ID and the account will only be active for the time period they need access to the system. Vendors will be assigned a generic ID due to the structure of the support organization. MY Consulting Inc., like other vendors, will be granted access only for the specific time necessary to address the issue.

3. VPN Access:

   User who have VPN access to the CLO servers utilizing their personal computers are required to have up to date Virus protection installed and running on their home computer. Virus software and version will be submitted to the IT director on an annual basis.

4. Screen Saver Enable or PC Lockout:

   a. PCs are configured to lock-out after being idle for 15 minutes, users are instructed to lock-out PC if leave the premises, otherwise the system will enforce to Lock-Out after 15 minutes.
   b. Users can resume activities by log back-in.

5. USB Blocked Devices:

   a) PC's are configured to block portable USB devices or removable hard drives; policy was implemented to deter to plug in removable hard drives that might compromise our network.
   c. If business requirements call to use USB removable hard drives, please send your request to ITSupport.clo.ok.gov stating the reason to access USB drives.