Data Classification Policy

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.

Classification

To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data will be classified into one of the following categories:

- Restricted data whose disclosure to unauthorized persons would be a violation of federal or state laws or Company contracts.
- Public data to which the general public may be granted access in accordance with the Company Contracts.

Data in both categories will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business, result in financial loss, or violate law, policy or Company contracts.

Security measures for data are set by the Chief Operating Officer (COO), working in cooperation with the operations staff, as defined below. The following roles and responsibilities are established for carrying out data policy:

- **Chief Operating Officer (COO):** Has responsibility for information management and is responsible for data access and policy implementation issues.
- **Operations Staff:** Are the data custodians. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by the COO or their designee, and implementing and administering controls over the information.

- **Data User:** Data users are individuals who need and use data as part of their assigned duties or in fulfillment of assigned roles or functions within the Company & Customer community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

Enforcement

Enforcement measures implemented for data security will be dictated by the data-classification level. Measures will include an appropriate combination of the following:

- Encryption requirements
- Data protection and access control
- Documented backup and recovery procedures
- Change control and process review
- Data-retention requirements
- Data disposal
- Audit controls
- Storage locations
- User awareness