InfoSafe
CERTIFIED

My Commitment to Privacy and Security

Big Mountain CPA is committed to meeting the information security expectations of its customers and protecting their right to privacy. To this end, I have adopted the **InfoSafe Certification** framework to ensure my cyber risk management and compliance procedures meet or exceed best practices.

A sample list of safeguards I have implemented and am maintaining, includes:

- **Security Awareness Training** - All personnel receive regular training and are tested on cybersecurity best practices for protecting sensitive information.
- **Network and Endpoint Protection** - Where possible, anti-malware software that automatically updates and performs regular security scans has been activated.
- **External Network Vulnerability Testing** - Compliance based network vulnerability tests are conducted at planned intervals to identify security threats.
- **Privacy Rights Management** - Policies and procedures have been established to comply with the requirements of applicable data privacy laws.
- **Physical Security** - Security measures are in place to prevent unauthorized access to buildings, offices, computer equipment and paper documents.
- **Access Controls** - Physical and electronic access to sensitive information is limited to only those personnel whose job duties require access.
- **Email Security/File Sharing** - Appropriate steps are taken to protect the transfer of sensitive information through the use of all types of communication.
- **Encryption** - Where possible, sensitive information is encrypted to prevent unauthorized access or disclosure.
- **Data Backup** - Technical measures are in place to ensure the continued availability of client data during adverse or disruptive events.
- **Secure Data Disposal** - Procedures are in place for the secure disposal of sensitive data and documents.
- **Vendor Risk Management** - Third party service providers that have access to sensitive information are required to follow appropriate cybersecurity practices.
- **Incident Response Planning** - Policies and procedures are established to ensure a quick, effective, and orderly response to information security incidents.
- **Third-Party Audit & Certification** - Cybersecurity policies, procedures, and security measures have been reviewed and certified by a third-party.
- **Employee Screening** - Employees are screened with reference checks and/or background checks prior to employment.

For more information about InfoSafe Certification, please visit www.infosafe.com.