THE BIONDO GROUP, LLC

DATA PROTECTION SUMMARY AND HIGHLIGHTS

The Biondo Group, LLC and its affiliates Biondo Investment Advisors, LLC and Biondo Wealth Services, LLC (collectively the 'Firm') maintains a Cybersecurity Plan that focuses on the protection of client, firm and employee confidential information. In establishing the Plan, the Firm performed a comprehensive risk assessment to determine areas in which controls needed to be established, enhanced or amended. The Firm focused on the protection and safeguarding of its network and systems, breach detection, electronic and physical access controls, third-party providers and vendor due diligence, employee training and response and recovery.

Below is a summarization of the Firm's efforts relating to the protection of its confidential information:

Cyber Security & Data Protection

The Firm protects against security threats and unauthorized access of electronic confidential information by:

- Employing a layered network security approach
- Utilizing a SIEM to store and monitor firewalls and server logs on a 24/7/365 basis
- Utilizing a SOC to respond appropriately to security events discovered by the SIEM
- Restricting access to the Firm's network and systems by 3rd party providers
- Reviewing activity on its network on a daily basis through its tracking software

The firms safeguards its electronic data by:

- Performing hourly and nightly backups to an on-site device and to 2 redundant storage facilities
- Utilizing password complexity with aging perimeters and forced password changes every 90 days
- Employing full disk encryption on all desktop and laptop computers with full server data file encryption
- Employing automated policy based email encryption
- Ensuring all mobile devices are protected through encryption and auto-lock

Physical Access Controls

The Firm's physical access controls include:

- An Intrusion Alarm System
- Secured server rooms with controlled accessibility
- Secured archive file room
- Secured offices during off business hours
- 'Clean desk' policy for all workstations
- Files secured nightly

Employee Training

All staff members are required to participate in training sessions, meetings and webinars, as determined by the Firm's Chief Information Security Officer. Training forums or tools include:

- Compliance Meetings
- Monthly Staff Meetings
- Ad hoc meetings
- Webinars
- Ad hoc testing
- Regulatory/Federal/State Bulletins & Releases
- Information and updates provided by IT

Response & Recovery

The Firm has established the following Plans relating to its response and recovery efforts:

- Data Security Incident Plan
- Incident Response Flow Chart
- Data Disaster Recovery Plan
- Business Continuity Plan

Cyber Liability Insurance

The Biondo Group currently maintains a $2,000,000.00 Cyber Liability Policy which has a $2,500.00 deductible.