# The Biondo Group, LLC Data Protection Summary & Highlights

The Biondo Group, LLC and its affiliates, Biondo Investment Advisors, LLC and Biondo Wealth Services, LLC (collectively the 'Firm'), maintains a Cybersecurity Plan (the 'Plan') that focuses on the protection of client, firm and employee confidential information. The Plan includes comprehensive risk assessments to determine areas in which controls need to be established, enhanced or amended. The Plan addresses the protection and safeguarding of the network and systems, breach detection, electronic and physical access controls, third-party providers, vendor due diligence, employee training, and response and recovery. Additionally, an external Penetration test is conducted annually to assess the overall security posture of the Firm's digital assets.

Below is a summary 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
- Utilizing DLP (data loss prevention) software on Endpoints (individual computers)
- Remote connectivity security protocols with Multifactor Authentication
- 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 two 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
- Utilizing WattBox to achieve automatic restart of servers in case of power disruptions
- 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
- Locked cabinet surrounding the server
- Secured archive file room
- Secured offices during off business hours
- 'Clean desk' policy for all workstations
- Files secured nightly

continued p2.

## 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:

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

## RESPONSE AND 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 with a $2,500.00 deductible.

January, 2024