# Steps we have taken to protect client information.

- ✓ Designate principal employee to manage cybersecurity policies and procedures.
- ✓ Install anti-malware and anti-virus software programs.
- ✓ Ensure that a hardware and software asset inventory is maintained and risk assessed.
- ✓ Identify and document asset vulnerabilities, internal and external threats.
- ✓ Identify potential business impacts.
- ✓ Develop procedures for responding to cybersecurity incidents.
- ✓ Develop back-up plans so critical business functions can continue.
- ✓ Establish alert procedures ensuring all employees know how to report any incidents or problems.
- ✓ Provide ongoing training for employees stressing due diligence in avoiding unintentional malware downloads and phishing emails.
- ✓ Be aware of all regulations regarding protection of information.
- ✓ Abide by SEC requirements to have policies and procedures for monitoring and overseeing vendors.
- ✓ Establish procedures to terminate employee access to information when no longer needed.
- ✓ Consider data encryption for all computers and mobile devices.
- ✓ Maintain list of 3rd party vendors and the information stored with them.
- ✓ Continue to protect client data stored with vendors until vendor access is revoked and data deleted.
- ✓ Use due diligence when contracting with cloud service providers.
- ✓ Assess the security of Wi-Fi connections when using mobile devices.
- ✓ Offer educational training seminars to clients.  Cyber threats may originate from clients.