10 Steps to Establishing a Cybersecurity Policy

Establishing a cybersecurity policy for a Registered Investment Advisor (RIA) involves several key steps. Here's a general framework to help you get started.

	SECURITY MEASURE	IN PLACE
1.	**Assess your current cybersecurity posture.**	
	Conduct comprehensive assessment of your current cybersecurity practices	❒
	Document any vulnerabilities and gaps	❒
2.	**Identify applicable regulations and best practices.**	
	SEC's Regulation S-P (Safeguarding Customer Information)	❒
	NIST Cybersecurity Framework or ISO 27001 industry best practices	❒
	GDPR (General Data Protection Regulation) if applicable	❒
3.	**Define scope and objectives.**	
	Identify systems, assets and data that will be covered	❒
	Establish specific objectives for your policy: - *Protecting client information* - *Maintaining data integrity* - *Ensuring business continuity*	❒
4.	**Establish governance and rules.**	
	Assign an individual or team to oversee and implement your cybersecurity policy	❒
5.	**Develop policy components.**	
	Information classification: *Define how information will be classified based on its sensitivity and establish appropriate controls for each classification level*	❒
	Access controls: *Outline procedures for granting and revoking access to systems and data, including strong authentication mechanisms and the principle of least privilege.*	❒
	Data protection: *Specify measures to protect data at rest, in transit, and in use, such as encryption, secure backups, and secure file transfer protocols.*	❒
	Incident response: *Define protocols for identifying, reporting, and responding to security incidents, including incident escalation, investigation, and communication procedures.*	❒
	Security awareness and training: *Establish requirements for educating employees about cybersecurity best practices and their roles in maintaining security.*	❒
	Third-party management: *Address how you will assess and manage the cybersecurity risks posed by third-party service providers and vendors.*	❒
	Mobile device management: *Establish policies and and usage guidelines to cover the three categories: bring your own, company owned/business only, company owned/personally enabled.*	❒

	SECURITY MEASURE	IN PLACE
6.	**Implement controls and safeguards.**	
	Next Gen endpoint detection and response	❒
	Firewalls	❒
	Multi-factor authentication	❒
	Patch management	❒
	Annual security assessments	❒
7.	**Communicate and educate.**	
	Schedule regular training and awareness sessions	❒
8.	**Incidence response planning.**	
	Processes for containing, investigating, and mitigating the impact of a breach or security event.	❒
9.	**Monitor and enforce compliance.**	
	Establish mechanisms to monitor	❒
	Review logs regularly	❒
	Conduct security assessments	❒
	Enforce established policies	❒
10.	**Regularly review and update**	
	Conduct periodic audits and assessments to ensure compliance with the policy.	❒

Remember that cybersecurity is an ongoing process, and it requires a proactive and continuous effort to stay ahead of emerging threats. It's advisable to seek expert guidance from cybersecurity professionals or legal advisors who specialize in regulatory compliance for RIAs to ensure your policy aligns with specific industry requirements.

For help with your cybersecurity policy or for a risk assessment, call us at 913.396.4600