COLORADO
Department of Regulatory Agencies
Division of Securities

Colorado Division of Securities – Cybersecurity Checklist

Written cybersecurity procedures should provide for:	**Y**	**N**
Identify Risks		
An annual assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Confidential Personal Information.		
Create an inventory of all computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers, and other equipment used by the firm.		
Locate and identify sensitive data and identify on which device(s) the data is stored. Also record which employee has access to the data.		
Identify client information transmitted via email, cloud services, firm websites, custodians and other third party vendors.		
Protect		
Establish authentication procedures for employee access to email on all devices (computer and mobile devices).		
Passwords for access to email are changed frequently (e.g. monthly, quarterly).		
Client instructions received via email are authenticated.		
Due diligence has been conducted on the cloud service providers, custodians and other third party vendors and evaluated as to whether the they have documented safeguards against breaches.		
All records are backed up off-site.		
Address data security and/or encryption requirements when transmitting information.		
Detect		
Use anti-virus software on all devices accessing the firm's network, including mobile phones. Anti-virus updates are run on a regular and continuous basis.		
Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events such as phishing and ransomware.		
Respond and Recover		
A plan and procedure in place to immediately notify authorities and clients in the case of a security incident or breach.		
A business continuity plan to implement in the event of a cybersecurity event.		
A process for retrieving backed up data and archival copies of information.		
Policies and procedures for employees regarding the storage and archival of information.		

Investment advisers and Broker-Dealers should review and comply with Division Cybersecurity Rules 51-4.14(IA) and 51-4.8.