Confidential Data Inventory

Definitions: Personal Identifying Information "PII" and Firm Sensitive Information – PII is any data that connects or identifies a specific person or business, which includes name, social security number, date and place of birth, mother's maiden name, or financial records including customer accounts and holding information. Firm Sensitive Information can include data such as contact information, email addresses, physical addresses, marketing plans, employee information, financial records, tax filings, etc. Firms can list data at a group level such as customer account information, or at the granular level such as social security number, customer name, date of birth, etc. (Please note: Definitions may vary by State.) ***Consider the questions below to determine where this information may be located within your firm and to address how it can be protected. Log the information into the chart below and maintain the inventory through routine internal cybersecurity risk assessments.

How is it captured? – What forms require the information? Is it included in multiple places? (i.e. Investment contracts, tax filings, custodian account forms)

Where is it physically/digitally located? – Where is the data stored? (i.e. files in a filing room, saved in a folder on the network drive, stored in a local file)

Who has access? – Who is able to view the data? (i.e. does the firm use the principle of least privilege?)

How is the data protected? – What steps does the firm take in order to secure the stored data? (i.e. encryption, password protected)

Is the data backed up? – Does the firm copy the data to be used in case of a cybersecurity incident? Does the firm initiate backups daily, weekly, annually?

Where are the backups located? – Does the firm store the backups on-site, offsite, in the cloud?

What is the confidential data?	How is it captured?	Where is it physically/digitally located?	Who has access?	How is the data protected?	Is the data backed up? If so, how often?	Where are the backups located?

What is the confidential data?	How is it captured?	Where is it physically/digitally located?	Who has access?	How is the data protected?	Is the data backed up? If so, how often?	Where are the backups located?