Constellation Research & Analytics' Data Security Protocols

GOAL:

- To ensure that our clients' donor data is handled safely and securely from the start to the completion of data analytics projects

SECURITY FRAMEWORK EMPLOYED:

- "Privacy by Design (PbD) is designed to reconcile the need for robust data protection with the desire for data-driven innovation. Developed in the late 1990s by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, PbD embeds privacy directly into the design specifications of technology, business practices and networked infrastructure." (Deloitte – https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/Analytics/ca-en-analytics-ipc-big-data.pdf)

- The principles for achieving this balance is: data minimization, de-identification, and user access controls.
    - **Data Minimization** – No personally identifiable information is collected unless a specific and compelling purpose is defined, all but eliminating privacy risk at the earliest stage.
    - **De-identification** – Datasets are stripped of all information that could identify an individual, either directly or through linkages to other datasets.
    - **User access controls** – A set of processes that grant or deny specific requests to obtain information; generally combined with other security policies.

- Potential Data Risks To Our Client and Its Donors Include:
    - Unauthorized disclosure, loss, or data theft (exacerbated when the data set contains identifiable information)
    - Managing accountability
    - Secondary use of data

- The Seven Principles of Privacy by Design Are:
    - 1. Use proactive rather than reactive measures; anticipate and prevent privacy invasive events before they happen.
    - 2. Personal data must be automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact.

- 3. Privacy must be embedded into the design and architecture of IT systems and business practices. It is not bolted on, after the fact.
- 4. All legitimate interests and objectives are accommodated in a positive-sum manner.
- 5. Security is applied throughout the entire lifecycle of the data involved.
- 6. All stakeholders are assured that whatever the business practice or technology involved, it is operating according to the stated promises and is subject to independent verification.
- 7. Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.

SECURITY PROTOCOLS TO ENSURE DATA SECURITY:

- ***Client-Vendor Kickoff Meeting***
  - Vendor will meet with the client to determine project goals and objectives in the information gathering meeting.
  - Data privacy risks will be discussed to identify potential security issues (data minimization, de-identification, user access controls).
  - Dataset scope and field selection will be discussed and decided upon by both the client and the vendor using PbD framework.

- ***Data Minimization***
  - No personally identifiable information (such as name, address, phone numbers, email addresses, etc.) will be collected or used for the project, unless by mutual agreement of the client and Constellation Research & Analytics for the specific purposes of the client project work. Only the information required to perform the work will be transmitted from the client to Constellation Research & Analytics.

- ***Data De-Identification***
  - Where feasible, datasets will be stripped of as much information as possible (given the scope of the project) that could identify an individual before the client transmits the data to Constellation Research & Analytics.
    - For data analytics projects, an index key will be created by the client to obscure the donors' identities but enable them to re-link the donor records back to the original dataset, which will protect the identities of the donors.
    - For wealth screening projects, only donor names and addresses are needed and will be used to perform the screening process. Screened donor records will then be uploaded back into the client's donor database. Further analysis often requires additional data points from

the client's donor records so Constellation Research & Analytics will employ the index key strategy and have the client export the needed information using the index key, thus protecting donor identities.

- ***User Access Controls & Transmission of Data***
  - The client will transmit donor data in an Excel Workbook with an encrypted password to the vendor's email.
  - The client will also send a second email containing the Excel Workbook password to the vendor.
  - The donor data will be saved onto an encrypted USB stick which will house the donor data while the data analysis project is being worked on. It will not be stored on a computer's hard drive. The file will be saved under a non-identifiable file folder name and the file's name will be changed to a non-identifiable name to obscure the true nature of the file.
  - The computer to be used will be Jason Ross' personal laptop, which resides at his home address only, and is equipped with NordVPN Threat Protection Pro (anti-malware and VPN).
  - When the project is complete, the file will be sent via email back to the client using password protection.