Security Document

1. How do you make sure the system is secure and data safe?
    a. This will involve a process of understanding what data is needed, along with having securities in place for data collection, storage, and visualization. Lastly, if this was real company personnel taking checks in the form of checking for vulnerabilities, security permissions on hardware, consulting with the legal team, and more.
2. What data is sensitive? (see here)
    a. The data collected will take the form of user email, ID, name (first and last name)
    b. Yes, this is Personal Identifiable Information (PII)
3. How will you protect it?
    a. There are a few different options available to us. First, is the overall recommendation is that upon the first entry/submission for new users this creates an account where the data is stored and then remembers the PII for future submissions. This could be secured safely for encryption. The next option is that upon submission, the data could be stripped or altered in order for it to not be traced back to the specific user (ex: stored for login, but just an appended ID number for each user could be leveraged) . Although, given this is for university-level there are permissions where they could obtain this user data, just not at our company level for legal reasons. Regardless, if this was not hypothetical and was a real business, we would need to consult a legal team.
4. What specific technologies will you use for protection? E.g., HTTPS.
    a. HTTPS will be a necessity on the user and admin panels to ensure the data is secure. Also, ensuring we have the necessary security permissions on the data warehouse used will be vital.