Information Security and Vulnerability Analysis

We understand that the data we will be processing and storing is highly confidential. In fact, nearly all the data will be confidential to a certain extent.

In the **"users" table**, we will be storing information on both faculty and users, which would represent a significant liability if this were leaked or improperly accessed. This information includes the user's full name, ID number, email address, and phone number. The NIST recognizes most of these as potential personally identifiable information (PII) because that can be combined with other data to identify a person.

The **"grades" table** of the database is also something that must be kept highly secure. Privacy of student grades is governed under the Family Educational Rights and Privacy Act (FERPA). Under this act, students have the right to reveal education records containing their grades. they also have the right to request correction of records they believe to be inaccurate, and if the school chooses not to amend the record, a formal hearing can be requested. For students under the age of 18 that are not attending an institute of higher education, the legal guardians of the students may exercise these same rights.

We will take several steps to provide a defense in depth approach to keeping this information safe and secure. This includes:

- **Sessions will timeout** after 15 minutes of inactivity.
    - Prevents unintended access to the account if the user forgets to logout.
- The website will utilize a **TLS 1.2 (HTTPS) certificate**.
    - TLS 1.2 is very secure and supported by all modern web browsers. This prevents man in the middle (MITM) attacks.
- **Input validation** will be used to prevent an attacker from tampering with the HTTP data on the front end, causing the database to return unauthorized data, such as that of another user.
    - This same principle will be applied to teachers and administrators. We must ensure the session ID matches the authenticated user to prevent students from tampering with their grades for example.
- The website and database will be tested against **other vulnerabilities and security best practices.**

Sources:

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html#:~:text=The%20Family%20Educational%20Rights%20and,privacy%20of%20student%20education%20records.&text=Parents%20or%20eligible%20students%20have%20the%20right%20to%20request%20that,to%20be%20inaccurate%20or%20misleading