Name: **Juliah Jane B. Gealon**

Secure Design Concept Paper (Work-in-Progress Submission)

1. Introduction

- Our capstone project is all about Outcome-Based Education System (OBE System). A system that is designed to track student progress, help the students to learn more by mapping each project outcome (PO) with Introductory, Enabling, and Demonstrative. Its main goal is to help the students to know where they excel and where they need to improve on a certain course. This can also help them once they graduate. The main goal is to ensure students achieve specific learning outcomes. For example, instead of saying "Students will learn programming," the outcome is "Students will be able to write and debug a simple computer program."

- Security is very important in the login module because it protects the system from people who are not allowed to enter. The login part is where users prove who they are, so if it is not secure, hackers can easily steal passwords or break into accounts. This can lead to stolen student data, changed grades, or damaged system files. By adding strong passwords, two-step verification, and data encryption, the system can make sure only real users can log in. A secure login keeps student information safe and helps maintain trust in the Outcome-Based Education (OBE) System. For our system it is a role-based access control, administrator, faculty, and student.

2. Application of Secure Design Principles

Secure Design Principle	Intended Application	Expected Benefit/Rationale
Least Privilege	Assign access rights based on user role (students, faculties, admins) so users only see or edit what they need.	Prevents unauthorized access or changes to sensitive student progress data.
Fail-Safe	Deny access to all system functions by default until the user is verified and given proper permissions.	Ensures only authorized users can access data, keeping the system settings secure.
Defense in Depth	Add multiple security layers such as input validation and authentication.	Protects the system from multiple attack points and reduces the risk of data breaches.

3. **Anticipated Risks and Controls**

Threat/Risk	**Potential Cause**	**Initial Control/Countermeasure**
Unauthorized Access	Weak authentication or shared password among users.	Apply multi-factor authentication and enforce unique, strong passwords for all users.
Data Loss	Lack of regular database backup or disaster recovery plan.	Schedule automatic database backups and store copies securely in the cloud.
Privilege Escalation	Improper role or permission configuration	Regularly audit user roles and permission to ensure least privilege is enforced.

4. **Compliance Consideration**
   - **Republic Act 10173 - Data Privacy Act of 2012**

     This law protects personal and sensitive information of individuals. For the OBE System, this means student records, grades, and learning progress must be stored and processed securely. I will apply this by encrypting student data, using secure login methods, and ensuring that only authorized users (like faculties and admins) can access sensitive information.

5. **Reflection**
   - **What did you learn from mapping security early?**

     I learned from mapping security early in the design of the OBE System security that it should be part of every stage of development, not just added at the end. It made me realize that adding security at the beginning saves time, effort, and resources. Planning security from the start helps identify possible threats, such as data leaks or unauthorized access, before they become bigger problems. Early security planning makes it easier to apply privacy laws, follow standards, and build user trust. The important thing I learned is that security should come first, not something added after.

   - **Which part of the design seems most challenging to secure, and why?**

     The most challenging part of the design to secure is the user authentication and data handling section. This is because it involves protecting sensitive information like usernames, passwords, and personal data from hackers. If this part is weak, attackers can easily gain access to the whole system.