System Security Assignment 3

"Our university is launching a new, all-in-one online portal. This portal will handle everything from student registration and grade management to faculty collaboration and research data storage. The system must protect student privacy, ensure academic integrity, and manage potential conflicts of interest among researchers."	**Tasks**
	1. Define the **security policy** for this portal.
	2. Identify **subjects** and **objects**
	3. Choose a primary **Access Control Model** or **Security Framework**
	4. Make an **Access Control Matrix**

Task 1: Define the Security Policy for the Portal

Since this portal has many aspects that require different security concerns, we will be using a combination of models.

1. **Bell-LaPadula:** → *The system must protect student privacy.*
    - Students should be able to view their own grades after results are released.
        - Students can't read other students' records.
    - Faculty members should be able to view students' registration data for students enrolled in their course.
        - Faculty can't write confidential student data in public areas.
    - Admins should be able to access all records for auditing purposes.
2. **Biba:** → *Ensure academic integrity.*
    - Students are able to submit assignments.
        - But they can't modify their grades.
    - Faculty members are able to enter and update grades.
        - But the grades can't be modified by lower users.
    - Admins can finalise grades at the end of the semester.
3. **Chinese Wall Model:** → *Manage potential conflicts of interest among researchers.*
    - A researcher uploads data for Project A (funded by Company X).
        - The same researcher later tries to access data from Project B (funded by Company Y, a competitor).
        - Once a researcher accesses Project A, they are blocked from accessing competing projects.
    - Faculty members collaborate on research documents within the same project.
        - Collaboration is allowed only within non-conflicting research groups.

Task 2: Identify Subjects and Objects

Subjects	Objects
• Student • Faculty Member • Researcher • Administrator	• Student Records • Grades Database • Course Materials • Research Data • Faculty Collaboration Space • System Configuration

Task 3: Choose Primary Access Control Model / Security Framework

Role-Based Access Control (RBAC) is suitable for this scenario because it allows for tasks that revolve around roles. For example, a student may read their records, grades, and material or a faculty member can read most things but write only the grades and course material for students. Assigning permissions based on roles would simplify access and while maintaining integrity and access management. It also integrates well with the hybrid security model from Task 1.

Task 4: Make an Access Control Matrix

Subject \ Object	Student Records	Grades	Course Materials	Research Data	System Config
Student	R (own)	R (own)	R	-	-
Faculty	R	R/W	R/W	R	-
Researcher	-	-	R	R/W (Chinese Wall)	-
Administrator	R/W	R/W	R/W	R/W	R/W