**Menal Noor**

**Topic: GRC Policy Kit – Sample Security Policies**

This project simulates a real-world compliance scenario by creating basic IT security policies mapped to international standards like NIST SP 800-53 and ISO 27001.

**1. Acceptable Use Policy (AUP)**

**Purpose:**

To define what users can and cannot do when using organizational IT resources.

**🧾 Policy:**

* Only use university or company systems for authorized purposes.
* Do not access malicious or inappropriate websites.
* Do not install unauthorized software.
* Do not share your login credentials.
* Report any security issues to the IT department.

**🧾 Framework Mapping:**

* NIST SP 800-53: AC-1 – Access Control Policy
* ISO 27001: A.9.1.1 – Access control policy

**2. Password Management Policy**

**Purpose:**

To ensure all users use secure, private, and strong passwords.

**🧾 Policy:**

* Passwords must be at least 8 characters with a mix of letters, numbers, and symbols.
* Do not reuse passwords across multiple accounts.
* Change passwords every 90 days.
* Never share your passwords with anyone.
* Avoid saving passwords in unsecured locations.

🧾 Framework Mapping:

* NIST SP 800-53: IA-5 – Authenticator Management
* ISO 27001: A.9.4.3 – Password Management System

**3. Data Classification Policy**

**Purpose:**

To categorize data based on its sensitivity and protect it accordingly.

**🧾 Policy:**

* Public Data: Can be shared openly (e.g., event flyers).
* Internal Data: Limited to authorized staff/students (e.g., internal reports).
* Confidential Data: Highly sensitive; must be encrypted and restricted (e.g., exam papers, student records).
* Data must be labeled accordingly and handled using proper controls.

🧾 Framework Mapping:

* NIST SP 800-53: PL-2 – System Security Plan, MP-4 – Media Storage
* ISO 27001: A.8.2.1 – Classification of Information

**Project Outcome:**

This policy kit demonstrates your ability to:

* Write formal security policies
* Align policies with international standards
* Understand real-world cybersecurity governance and compliance practices