Mobile Device Management (MDM) Policy

Objective: Create a **Mobile Device Management Policy** to ensure that company devices are used securely.

Steps:

1. **Understand the Importance of MDM**:
    - Explain the need for controlling and securing mobile devices (e.g., smartphones, tablets) used to access company data.
    - Discuss the risks of **BYOD (Bring Your Own Device)** policies and the need for **Mobile Device Management** (MDM).

2. **Drafting an MDM Policy**:
    - Interns will draft a **Mobile Device Management Policy** that covers:
        - Enrollment of devices into the company's MDM system.
        - Security requirements for mobile devices (e.g., strong passwords, encryption, remote wipe capability).
        - Guidelines for accessing company resources via mobile devices (e.g., VPN, use of secure apps).
        - Procedures for handling lost or stolen devices.

3. **MDM Scenario**:

MDM Scenario: Lost or Stolen Mobile Device

Scenario: An employee at XYZ Corp, Sarah, is attending a business conference and accidentally leaves her mobile device unattended in a public area. Upon realizing it is missing, Sarah immediately contacts her supervisor to report the situation. The device contains sensitive company data, including emails, documents, and access to internal systems.

Task for Interns: Outline the immediate actions required to address this situation. Consider the steps for securing company data, reporting the incident, and recovering the device.

Key Actions to Address:

1. **Reporting**: Sarah should immediately report the incident to the IT department or designated security team.
2. **Remote Wipe**: The IT team should initiate a remote wipe of the device to erase all corporate data.
3. **Device Tracking**: If possible, use device tracking software to locate the mobile device.
4. **Change Credentials**: Sarah should change any passwords associated with corporate accounts, especially if login credentials were stored on the device.
5. **Update Incident Records**: The IT department should document the incident for internal reporting and potential security review.
6. **Informing Stakeholders**: If necessary, notify the relevant internal stakeholders or external authorities (e.g., law enforcement) about the loss of the device.

Please describe these actions in detail and explain why they are crucial for securing sensitive company data.

Deliverables:

- A **Mobile Device Management Policy**.
- A short report detailing the steps the company should take in the event of a lost or stolen device.