**Purpose:**
To show that I can design an Intune device compliance policy which is an essential part of securing devices that connect to Microsoft 365 services.

## Structure & Content

**Title:**
**Planned Device Compliance Policy and Secure Device Access**

**Objective:**
To ensure only secure and compliant devices (managed through Intune) can access Microsoft 365 resources.

**Background:**
Device compliance policies validate that devices meet certain security requirements (e.g., encryption, passcode, no jailbreaking).
When combined with Conditional Access, they help enforce Zero Trust principles.

**Planned Policy Configuration:**

| Setting | Description |
|---|---|
| **Policy Name** | Require Compliant Device for Exchange and SharePoint |
| **Platform** | Windows 10 and later (example) |
| **Compliance Requirements** | - Require BitLocker encryption<br>- Require password or PIN<br>- Minimum OS version (Windows 10 22H2)<br>- Device must not be jailbroken/rooted |
| **Actions for Noncompliance** | Block access to Microsoft 365 apps |
| **Reporting & Monitoring** | Device compliance reports in Intune Admin Center |

**Expected Behavior:**
If a device is noncompliant (e.g., lacks encryption), access to Exchange Online and SharePoint will be blocked until compliance is restored.

**Screenshot References:**

- planned_compliance_policy.png - Intune policy configuration page

**Outcome:**
Documenting this policy shows understanding of Intune compliance configurations and how device-based access conditions work within Microsoft 365 security.