Accessing Email & More on Your Mobile Device

Microsoft 365 App Protection Policies

Overview: To better protect the data living within the Microsoft 365 (M365) Mobile Apps, a new security feature is being implemented called App Protection Policies. This applies to Outlook, One Drive, Teams, Microsoft Office (Excel, Word, PowerPoint) and additional M365 apps. The App Protection policies get applied to the data in the applications, but leave the device settings untouched. This means that we can protect the GMHEC data without the need to manage a device, only the data in the M365 apps.

How do you prepare your mobile device for Mobile App Protection Policies?

- Install the **Intune Company Portal** app on your iOS or Android mobile app and sign into the Company Portal App.
    - The Company Portal app is required so the apps on your device can talk to the policy settings in M365.
- When you open a M365 mobile app, you will be asked to restart the app. “Your organization is protecting the application and it must be restarted.”
- You will be required to setup a PIN. After you set the PIN, you can also use your fingerprint or face ID to unlock the apps to use them.

How will this affect the use of these apps on mobile devices?

- When the policies are implemented, you will be required to set a PIN to access the M365 apps.
- Data will not be able to be copied out of a M365 app and moved into a non-M365 app. For instance, you are not able to copy text out of Word or Outlook and paste it into the Gmail App.
- You will be able to bring data into the M365 apps from any source. Once the data is in the M365 apps, it can be used between the apps without issue.

Additional Information References

- App protection policies overview - Microsoft Intune | Microsoft Docs