Digital Workspace | Secure Data on Personal Devices

IMPLEMENTATION DELIVERABLES

- Verify all Prerequisites are in place for Implementation of Microsoft Intune Application Protection Policies
- Identify and Document Customer Specific App Protection Policies using the Microsoft Data Protection Framework as a Baseline
- User Impact Documentation
- Create and Deploy up to five Microsoft Intune App Protection Policies and Target the Pilot Users Group
- Modify App Protection Policies, as necessary, within five days of Initial Deployment
- Implement an Entra ID Conditional Access Policy to force Pilot Users through Microsoft 365 Mobile Apps only

ASSUMPTIONS

- iOS/iPadOS/Android Devices targeted for Microsoft Intune app protection policies meet the minimum requirements for running the latest available version of the Microsoft 365 applications.
- All user piloting and deployment tasks will take place in the Customers production tenant.
- The User Principal Name (UPN) assigned to users in Windows Server Active Directory must be routable.
- Users protected by app protection policies targeting Outlook have mailboxes hosted on Exchange Online only.
- Users targeted for app protection policies targeting Word, Excel or PowerPoint must have a Microsoft 365 apps for business or enterprise license assigned.
- Users do not have more than one “corporate” identity configured on their mobile applications being targeted for app protection policies.

NON-DELIVERABLES

- Direct end user support. CDI will provide tier-3 support to the Customers IT staff only.
- Enrollment of devices in any device management solutions such as Microsoft Intune
- Production deployment to users/devices beyond the pilot user scope (maximum 20 users)
- Deployment of app protection policies targeting any non-Microsoft 365 applications.
- Application of app protection policies to the Skype for Business mobile application
- Deployment, configuration, or integration of Microsoft Intune mobile threat defense (MTD) solutions.