Microsoft Intune Device Management SOP

Purpose

To establish a legally sound, standardized procedure for using Microsoft Intune to manage issued devices. This includes enrollment, remote actions, compliance enforcement, report analysis, incident notifications, and app management. Covers all laptops, desktops, tablets, and mobile phones issued, managed under Microsoft 365 Business Premium via Microsoft Intune.

1. User Permissions

|  |  |  |
| --- | --- | --- |
| **Task** | **Required Role** | **Access Location** |
| Enroll a device | User or Intune admin | Company Portal app (user) or Intune admin center > Devices > Device onboarding (IT) |
| Assign compliance policy | Intune or Endpoint Security admin | Intune admin center |
| Run remote wipe/lock/retire | Intune/Global admin | Device page in Intune admin center |
| View device reports | Intune admin | Intune admin center > Reports |
| Check location | Intune admin | Device page > Locate device |
| Configure app deployment | Intune admin | Intune admin center > Apps |
| Access audit logs | Global admin | Intune admin center > Users > Audit logs |

1. Device Enrollment
2. Windows Devices (Autopilot)
3. Register the device hardware hash via Devices > Device onboarding > Enrollment > Devices.
4. Assign device to an Autopilot deployment profile via Deployment profiles.
5. Assign primary user under Devices > Properties > Primary user.
6. macOS/iOS/Android
7. For Apple: Enroll via Apple Business Manager.
8. For Android: User Android Enterprise with Work profile.
9. For BYOD: Require Company Portal app installation and manual sign-in.

NOTE: BYOD devices require user consent and onboarding agreement before enrollment.

1. Compliance Policies and Notifications
2. Go to Devices > Compliance and create a new policy.
3. Assign policies to device/user groups.
4. View compliance status in Reports > Device compliance.
5. Notifications can be added by going to Compliance > Notifications > Create notification.

NOTE: Devices can be restricted from accessing corporate data if non-compliant via Conditional Access (see below on Conditional Access).

1. Remote Actions
2. Go to Devices > [Select Device].

|  |  |  |
| --- | --- | --- |
| **Action** | **Use Case** | **Legal Conditions** |
| Wipe | Lost/stolen device | Company-owned devices only |
| Retire | BYOD separation | Consent required |
| Lock | Suspected misuse or theft | Only on managed devices |
| Restart | Troubleshooting or patching | Logged and tracked |

1. Reports and Device History
2. Go to Devices > [Select Device] > Overview
3. Check for:

* Last check-in time
* Primary user
* Enrolled by
* Compliance

1. Go to Device compliance to check how the device meet’s established policies.
2. Go to Managed Apps to check device’s compliance with required apps, app wipes, etc.
3. To view all devices for a user, go to Users > [Select User] > Devices.
4. App Deployment
5. Go to Apps > All Apps and add an application by clicking Create.
6. Assign to user or device group.
7. Choose install behavior (either required, available, or uninstall).
8. Track install success/failure from app dashboard.
9. Location Tracking
10. Go to Devices > All devices > [Select Device] > Locate device.

NOTE: Only permitted on org-owned devices. Users must be informed during onboarding.

1. Conditional Access Policies

Use cases include requiring MFA when off-site, blocking access from non-compliant devices, and/or restricting to trusted IPs only.

1. Go to Endpoint security > Conditional access and click on New Policy.
2. Assign users and groups as well as target apps.
3. Set conditions, such as sign-in risk, location, and device platform.
4. Configure access control, including requiring MFA or compliant devices, and blocking access if requirements aren’t met.
5. Start in Report-Only mode, then switch to On.
6. To monitor impact of conditional access policies, go to Users > Sign-in logs.
7. Notifications
8. Go to Device > Compliance > Notifications.
9. Trigger email to IT for enrollment failure, compliance failure, encryption not enabled, etc.
10. Custom Terms of Use
11. Go to Endpoint security > Conditional access > Terms of use and create a new Terms of Use.
12. Upload a document that includes policies on device tracking, remote wipe, data handling, compliance enforcement, and user responsibilities.
13. Configure display settings such as display name, requiring users to consent, expiration consent, and language.
14. Create a new policy to assign Terms of Use.
    1. Go to Conditional access > Policies and create a new policy.
    2. Target is all users or specific groups and require Terms of Use for access controls.

NOTE: Terms should be reviewed by HR/legal before enforcement.

1. Endpoint Security Baselines
2. Go to Endpoint security > Security baselines and choose a baseline.

* Microsoft Defender for Endpoint (if licensed)
* Windows 10 Security Baseline (most used)
* Microsoft Edge Baseline (for browser lockdown)

1. Create policy and configure settings.
   1. Review each category (e.g., BitLocker, Defender AV, Credential Guard).
   2. Adjust settings only if needed (default recommendations are strong).
2. Assing to a group, review, and create.
3. To view policy success/failure by device, go to Endpoint security > Monitor > Assignment failures.
4. Application Protection Policies
5. Go to Apps > Manage apps > Protection and create a new policy.
   1. Choose the platform you’re creating a policy form. Have a different policy for each platform.
6. Select target apps: Outlook, Teams, OneDrive, etc.
7. Configure data protection settings.

|  |  |
| --- | --- |
| Setting | Recommended |
| Prevent backup | Yes |
| Encrypt app data | Yes |
| Restrict copy/paste | Block between apps |
| Require PIN | Yes |
| Wipe after failed PIN | 5 attempts |

1. Configure access requirements.
   1. Require PIN or biometric, recheck access after timeout, and block rooted/jailbroken devices.
2. Assign to users or groups.
3. To monitor, go to Apps > Monitor > App protection status.

This SOP must be reviewed every six months or upon major policy or procedural changes.