INTUNE POLICIES

# Contoso Legal LLP

Harbour IT

| PREPARED BY | DATE | DATA COLLECTED | MICROSOFT 365 TENANT |
|---|---|---|---|
| Harbour IT | 29 Nov 2026 | 29 Nov 2026, 10:48 UTC | contoso.onmicrosoft.com |

Which platforms have a compliance policy, what each compliance policy requires, configuration profiles and Windows update rings, endpoint security policies and app protection for phones, with whom each applies to.

**Filtered view.** Needs attention: 3 of 7 rows, Flag is Medium. Configuration profiles: 4 of 4 rows, 1 column hidden. The headline figures cover every row.

Compliance policies
**2**
1 assigned to someone

Platforms without compliance
**1**
Devices enrolled, no compliance policy

Policies assigned to nobody
**3**
Policies that do nothing until assigned

Update rings paused
**1**
Of 2 Windows update rings

App protection
**iOS and Android**
1 enrolled phone; personal phones count too

## Coverage by platform 3 1 to review

For each platform, the devices enrolled in Intune and how many policies assigned to someone cover it. A device with no compliance policy counts as compliant unless Intune's compliance settings say otherwise, so Conditional Access can't tell it apart.

| Flag | Platform | Enrolled devices | Compliance policies | Configuration profiles | Endpoint security and settings catalog | App protection |
|---|---|---|---|---|---|---|
| | Windows | 19 | 1 | 3 | 1 | – |
| Medium | iOS/iPadOS | 1 | 0 | 0 | 0 | 1 |
| | Android | 0 | 0 | 0 | 0 | 1 |

## Needs attention 3 3 to review

Policies that do nothing or leave a gap, and platforms with devices but no compliance policy.

| Flag | Policy | Kind | Platform | What to check |
|---|---|---|---|---|
| Medium | Android Outlook | App protection | Android | No PIN to open company apps |
| Medium | iOS/iPadOS | Platform | iOS/iPadOS | Devices are enrolled but no compliance policy is assigned (1 device) |
| Medium | Update ring Pilot | Update ring | Windows | Security updates paused |

## Compliance policies 2

What a device must meet to count as compliant. Conditional Access can then let only compliant devices reach company data.

| Flag | Policy | Platform | Requires | Assigned to | Last changed |
|---|---|---|---|---|---|
| Low | iPhone draft | iOS/iPadOS | Password of 6+ characters, Not jailbroken or rooted | Nobody | 1 Feb 2026 |
| | Windows baseline | Windows | Password of 8+ characters, BitLocker, Secure Boot, Microsoft Defender on, Version 10.0.22631 or later | All devices | 14 Aug 2026 |

## Windows update rings 2 1 to review

How long Windows waits before installing monthly security updates and yearly feature updates, and how long before it restarts to finish them. Microsoft suggests no more than 7 days for security updates on most devices.

| Flag | Ring | Security updates after (days) | Feature updates after (days) | Restart deadline (days) | Paused | Drivers | Assigned to |
|---|---|---|---|---|---|---|---|
| | Update ring Broad | 7 | 60 | 3 | No | Included | Sales, Except Project Phoenix |
| Medium | Update ring Pilot | 0 | 0 | 2 | Security | Left out | Board (filtered) |

## Configuration profiles 4 1 to review

Settings Intune pushes to devices. Settings shows the ones that matter most for security.

| Flag | Profile | Type | Platform | Assigned to | Last changed |
|---|---|---|---|---|---|
| Low | Mac restrictions | Device restrictions | macOS | Nobody | 1 Apr 2026 |
| | Update ring Broad | Update ring | Windows | Sales, Except Project Phoenix | 1 May 2026 |
| Medium | Update ring Pilot | Update ring | Windows | Board (filtered) | 30 Sep 2026 |
| | Windows firewall | Endpoint protection | Windows | All devices | 10 Jan 2026 |

## Endpoint security and settings catalog 2

Endpoint security policies (antivirus, firewall, disk encryption and the like), security baselines and settings catalog profiles.

| Flag | Policy | Kind | Platform | Settings | Assigned | Last changed |
|---|---|---|---|---|---|---|
| | Defender antivirus | Antivirus | Windows | 14 | Yes | 1 Jul 2026 |
| Low | Mac FileVault | Disk encryption | macOS | 3 | No | 1 Apr 2026 |

## App protection for phones 2 1 to review

Rules for company data inside apps such as Outlook and Teams on phones, including personal phones Intune doesn't manage: a PIN to open them, and whether data can leave for other apps.

| Flag | Policy | Platform | PIN | Sharing data | Copy and paste | Backups | Encryption | Apps | Assigned to |
|---|---|---|---|---|---|---|---|---|---|
| Medium | Android Outlook | Android | Not required | With any app | Any app | Allowed | Encrypted | 2 | Sales |
| | iOS Outlook and Teams | iOS/iPadOS | Required (6+ digits) | Managed apps only | Managed apps (paste in from any) | Blocked | When locked | 4 | All users |

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 29 Nov 2026, 10:48 UTC.