IBM Security
創新思維領導白皮書

自攜裝置 (BYOD) 的十個規定

瞭解當使用者使用個人裝置處理公務時如何保護公司資料

IBM

您是否應該允許 BYOD？

對許多 IT 主管而言，行動裝置進入工作環境後迅速大量增加的現象看似有如神助。行動裝置及其應用程式已徹底顛覆我們的生活方式 - 包含我們的溝通、旅行、購物、工作與更多方面。這樣的行動力轉型如此徹底、如此劇烈，我們現在都難以想像沒有這些裝置的生活。自攜裝置 (BYOD) 就此應運而生，而員工就追隨這樣的潮流。

假裝什麼事都沒有發生或是說「我們不會讓員工這麼做」，沒有任何意義。事實是，他們已經這麼做了，而且可能在您允許/不允許的情況下，持續讓不符合規定的裝置偷渡到網路。在 2016 年之前，大多數的企業員工都能使用自己的智慧型手機和平板電腦來處理公務。

這造成了不可避免的問題：您如何支援工作人員想要使用個人應用程式和裝置的需求，同時還能讓他們在能保護公司資料的安全環境中保持生產力？ *自攜裝置 (BYOD) 的十個規定* 讓您瞭解如何建立平靜、受保護且有生產力的行動環境。

自攜裝置 (BYOD) 的十個規定

1. 先制定您的政策，然後再採購技術
2. 尋找可存取公司資源的裝置
3. 註冊應該要很簡單
4. 以無線方式設定裝置
5. 協助您的使用者幫助自己
6. 讓個人資訊保持私密
7. 將個人資訊與公司資料分開
8. 管理資料使用情況
9. 持續監控裝置是否違反規定
10. 享受 BYOD 帶來的投資報酬率

1. 先制定您的政策，然後再採購技術

如同任何其他 IT 專案，政策必須優先於技術 - 當然，在雲端中也是如此。若要有效地使用行動裝置管理 (MDM) 技術來管理員工自有裝置，您仍然需要制定政策。這些政策影響的範圍不僅是 IT；還會影響人資、法務和保全，以及任何基於生產力而使用行動裝置的公司部門。

因為所有業務線都會受到 BYOD 政策的影響，所以不得只由 IT 部門制定。基於使用者的多元需求，IT 必須確保制定政策時會將他們納入考量。

沒有一體適用的適當 BYOD 政策，但有下列問題需要考量：

- **裝置：** 要支援哪些行動裝置？只支援特定裝置，或是員工需要的任何裝置呢？
- **資費方案：** 組織是否會全額支付資費方案的費用？您是否會發出津貼，或是員工是否會提交支出報告？
- **合規性：** 哪些法規會規範您組織需要保護的資料？例如，《健康保險隱私及責任法案》(HIPAA) 要求任何裝置若持有受制於該法案的資料，就必須要具備原生加密。
- **安全性：** 需要哪些安全性措施 (密碼保護、破解/刷機的裝置、防惡意程式應用程式、加密、裝置限制、iCloud 備份)？
- **應用程式：** 哪些應用程式會遭到禁止？IP 掃描、資料共用、Dropbox？
- **協議：** 是否有「可接受使用量協議」(AUA) 加諸於裝載公司資料的員工裝置？
- **服務：** 員工可以存取哪些種類的資源 - 電子郵件？特定的無線網路或 VPN？CRM？
- **隱私權：** 會從員工的裝置收集哪些資料？絕對不會收集哪些個人資料？

談到 BYOD 時，沒有問題是不能提出的。關於裝置的使用方式和 IT 會如何確實滿足那些需求，所有對話都應該坦白和誠實以對。

2. 尋找可存取公司資源的裝置

想像一下。您開始使用 MDM 解決方案 - 假設您的公司支援 100 個左右的裝置。您持有一份很詳細的裝置類型和使用者資料的試算表 – 這應該沒什麼好大驚小怪的。但是，當您首次檢視報告時，其中有超過 200 多個裝置。這樣的情況確實存在，而非虛構。比您想像地更常發生。

別急著否認。不知道事實真相可能會有危險。先瞭解行動裝置數量的目前狀況，然後再制定您的策略。若要落實此目標，您需要能與電子郵件環境持續溝通並偵測與公司網路連線之所有裝置的工具。請記住，針對信箱開啟 ActiveSync 之後，在 IT 不知情的情況下，同步處理多個裝置通常不會有任何阻礙。

必須將所有行動裝置整合至您的行動先導計畫，而且必須通知其擁有者，新的安全性政策即將實施。

3. 註冊應該要很簡單

複雜性往往容易造成不合規的情況。當您識別出要註冊的裝置之後，BYOD 方案應該使用能讓使用者簡單輕鬆註冊裝置的技術。此程序應該簡單且受到保護，並在同一時間設定裝置。

在完美的情況下，使用者應該要能夠前往電子郵件連結或遵循文字來到在其裝置上建立的 MDM 設定檔 - 包含接受有史以來最重要的 AUA。

將 BYOD 視為與 AUA 的結合 - 作為可支持和諧婚姻的婚前協議書。

指示應該協助現有使用者註冊 BYOD 方案。建議現有使用者清除其 ActiveSync 帳戶，如此您就能隔離和管理裝置上的公司資料。新裝置應該從使用全新的設定檔開始。

從 IT 觀點看來，您需要能大量註冊現有裝置的能力，或是讓使用者自行註冊其裝置。您也需要使用基本驗證程序 (例如，一次性密碼) 或使用現有公司目錄 (例如，Active Directory/LDAP) 來驗證員工。嘗試存取公司資源的任何新裝置都應該予以隔離和通知 IT。這可讓 IT 彈性地封鎖或初始化適當的註冊工作流程 (若獲得核准)，從而協助確保遵循公司政策。

4. 以無線方式設定裝置

如果有 BYOD 政策及 MDM 解決方案不應該做的事，那就是讓更多使用者跑到服務台尋求協助。您的裝置應該能無線設定，才能同時讓 IT 及企業使用者徹底發揮效率。

使用者接受 AUA 之後，您的平台應該提供員工存取下列項目時所需的所有設定檔、認證和設定：

- 電子郵件、聯絡人和行事曆
- VPN 和 Wi-Fi
- 公司文件及內容
- 內部及公用應用程式

目前，您也能制定政策以限制特定應用程式的存取權，並在使用者超過資料使用量或當月津貼限額時產生警告。

5. 協助您的使用者幫助自己

而且，我們會對您的所作所為感激不已。使用者想要能發揮功能的裝置，而您希望最佳化服務台時間。穩健強大的自助平台可讓使用者直接執行：

- 員工忘記現在密碼時，重設 PIN 及密碼
- 從 Web 入口網站使用地圖整合，找到遺失裝置的地理位置
- 遠端抹除裝置、移除敏感性公司資料

安全性、公司資料保護及合規性是共同的責任。這對員工而言可能是必要之惡，但沒有員工的配合，就無法緩解風險。自助服務入口網站可協助員工瞭解他們為何可能違反規定。

6. 讓個人資訊保持私密

當然，BYOD 政策不只是保護公司資料，精心構思的 BYOD 方案能防止其他人 (包含 IT 在內) 存取員工個人資料。個人可識別資訊 (PII) 可用於識別、聯絡或找到人員。某些隱私權法律可防止企業檢視此資料。和員工溝通隱私權政策的內容，讓他們清楚瞭解您無法從其行動裝置收集的資料。例如，MDM 解決方案應該能剖析其可存取和無法存取的資訊，例如：

- 個人電子郵件、聯絡人和行事曆
- 應用程式資料和文字訊息
- 通話記錄和語音郵件

換句話說，要讓使用者瞭解您收集的資料、其使用方式，以及他們為何能從中獲益。

進階的 MDM 解決方案可將隱私權政策轉化為隱私權設定，以隱藏裝置上的位置和軟體資訊。這可協助公司符合 PII 規範並讓員工更加自在，因為這可防止他人檢視智慧型手機和平板電腦上的個人資訊。例如：

- 停用應用程式庫存報告，以限制管理員檢視個人應用程式。
- 停用定位服務，以防止存取實際地址、地理座標、IP 位址和 Wi-Fi SSID 等位置指標。
- 透明度及清晰度也是重要的口號。如果每個人都瞭解規定的內容，BYOD 政策遇到的抵抗就會減少。

7. 將個人資訊與公司資料分開

若要讓 BYOD 成為 IT 及使用者都能認可的協議，應該將生日派對照片或偉大的美國小說等個人資訊與生產力應用程式區隔開來。

簡單來說，公司應用程式、文件和其他資料必須由 IT 保護，如果員工決定離開組織，公司 IT 也不應該碰觸個人電子郵件、應用程式和照片。

不僅使用者會喜歡這方法帶來的自由，IT 也會這麼想，因為他們的工作會因此輕鬆許多。使用此方法，如果員工從公司離職時，IT 可以選擇性地只抹除公司資料。視情況而定，如果員工遺失裝置，也可以抹除整個裝置內容。真正的 MDM 解決方案可為您提供這樣的選項。

估計有 86% 的裝置抹除是選擇性的，只會抹除公司資料。

8. 管理資料使用情況

BYOD 政策可在很大程度上讓 IT 無需參與溝通討論過程，但許多公司仍需要協助員工管理其資料使用，以避免產生超額費用。

如果您支付資費方案的費用，則需要方法來追蹤此資料。如果您並未付費，則可能需要協助使用者追蹤其目前的資料使用量。您應該能夠追蹤網路內和裝置上的漫遊資料使用量，如果使用者超過資料使用量，則會產生警示。

您可以設定漫遊和網路內 MB 限制並自訂結帳日，以根據使用比率來建立通知。建議您教育使用者瞭解使用 Wi-Fi (若可用) 的好處。自動 Wi-Fi 配置有助於確保在公司所在位置時，裝置會自動連線至 Wi-Fi。

如果津貼計畫每月只補貼 50 美元或 200 MB 的資料使用量，員工可能會很感謝您發出費用即將超額的警告。

9. 持續監控裝置是否違反規定

裝置註冊之後，就全部是內容的問題了。在特定情況下，應該持續監控裝置，而且應該已制定自動化政策。使用者是否嘗試停用管理？裝置是否符合安全性政策？您是否需要根據所見的資料來進行調整？您可以從此處開始瞭解其他政策或是要建立的規定。以下是幾個常見問題：

- **前往破解的根源：** 為了免費取得付費應用程式，員工有時候會對手機進行「破解」或「刷機」動作，打開通往惡意程式的大門而導致資訊遭竊。如果裝置遭到破解，MDM 解決方案應該能採取行動，例如選擇性地立即抹除裝置的公司資訊。
- **不必在裝置上滑動；傳送簡訊：** 如果「憤怒鳥」這類打發時間的應用程式違反公司政策，但不屬於犯罪行為，則自動抹除可能過於嚴厲。MDM 解決方案可根據違規內容而強制執行政策。MDM 可以傳送訊息給使用者，讓他們有時間在 IT 抹除資訊之前，先行移除應用程式。
- **有新的作業系統可用。** 若要讓 BYOD 維持有效狀態，當有新的作業系統可供安裝時，使用者需要簡單的方法獲得通知。有了適當的 MDM 解決方案，作業系統升級就能變成自助服務功能。限制過期作業系統版本有助於確保合規性和最佳化裝置可操作性。

10. 享受 BYOD 帶來的投資報酬率

由於 BYOD 會將購買裝置的責任轉移到員工身上，所以值得您考慮組織的整體願景和長期成本。

在撰寫政策時，考量政策會對投資報酬率造成何種影響。那包含比較方法，如下所示：

公司財產模式

- 您願意對每個裝置花費多少成本
- 完全補助資費方案的成本
- 每隔幾年回收裝置的成本
- 保固計畫
- 用於管理方案的 IT 時間和人力

BYOD

- 部分補助資費方案的成本
- 消除的裝置採購成本
- 行動管理平台的成本

雖然無法一體適用，但精心構思的 BYOD 政策可引導您有效果且有效率地邁向管理行動裝置的方向。

當然，當員工能隨時保持行動和連線狀態，通常就能提升生產力。BYOD 是利用這項進展提升新使用者生產力的絕佳方式，因為這類使用者之前可能還不符合持有公司裝置的資格。

BYOD：自由的安全性

BYOD 是新興的最佳作法，可讓員工享有使用自有裝置處理公務的自由，同時還能減輕 IT 重大的財務和管理負擔。但是，如果沒有精心構思的政策和穩健強大的管理平台，BYOD 將無法實現這些簡化管理及節省成本的承諾。

如果您仍然處於制定行動策略的早期階段，IBM® MaaS360® 提供許多教育資源。

如果您認為 BYOD 符合您的企業需求，按一下此處 即可免費體驗 MaaS360 的 30 天試用版。因為 MaaS360 是雲端型裝置，您的測試環境會自動成為生產狀態且不會遺失資料。

關於 IBM MaaS360

IBM MaaS360 是企業行動力管理平台，可針對人員工作的方式啟用生產力及資料保護。數萬個組織都相信 MaaS360 能作為其行動力先導計畫的基礎。MaaS360 提供全方位管理以及跨使用者、裝置、應用程式及內容之間的堅實安全性控制力，以支援任何行動部署。如需 IBM MaaS360 的詳細資訊並開始使用免費 30 天試用版，請造訪 www.ibm.com/maas360

關於 IBM Security

IBM 的安全性平台提供安全性智慧，以協助組織全面保護其人員、資料、應用程式及基礎架構。IBM 提供解決方案以用於身分識別及存取管理、安全性資訊和事件管理、資料庫安全性、應用程式開發、風險管理、端點管理、新一代入侵保護及其他。IBM 營運全球最廣泛安全性研究及發展和交付組織之一。如需更多資訊，請造訪 www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美國印製 2016 年 3 月

WGW03112-TWZH-01