IBM Security
思维领导力白皮书

自带设备的十大规则

了解用户将个人设备用于工作时如何保护公司数据

IBM

是否应该允许 BYOD?

进入工作场所的移动设备快速激增，对于许多 IT 主管而言如有神助。移动设备及其应用程序改变了我们的生活方式 — 我们的沟通、旅行、购物、工作等各个方面发生了天翻地覆的变化。这场移动性变革如此彻底，波及范围如此之广，让人很难想象没有这些设备，我们会陷入怎样的境况。自带设备 (BYOD) 应运而生，并且受到了员工们的追捧。

假装这种情况没有发生或者说“我们不会让员工这样做”是没有任何意义的。事实上，他们已经这样做了，而且很可能在获得或未获得您允许的情况下，继续将不符合安全要求的设备带入您的网络。到 2016 年，绝大多数的企业员工都将获准使用自己的智能手机和平板电脑进行工作。

这样就带了了一个不可避免的问题：您如何做到既支持员工使用个人应用程序和设备的愿望，又让他们在保护企业数据的安全环境下高效工作？ *自带设备的十大规则* 向您展示如何创建平静、安全且高效的移动环境。

自带设备的十大规则

1. 采购技术之前先制定政策
2. 找出访问公司资源的设备
3. 注册应该简单
4. 远程配置设备
5. 帮助用户自助
6. 个人信息保密
7. 将个人信息与公司数据分开
8. 管理数据使用情况
9. 持续监控设备防止出现不合规
10. 坐享 BYOD 带来的投资回报 (ROI)

1. 采购技术之前先制定政策

正如任何其他 IT 项目一样，政策必须走在技术前面 — 是的，即使在云端也应如此。要想高效使用移动设备管理 (MDM) 技术管理员工自有设备，您仍然需要确定政策。这些政策影响的不仅仅是 IT；它们还会影响人力资源、法律和安全 — 以生产力名义使用移动设备的任何业务部分。

由于所有业务部门都会受到 BYOD 政策的影响，所以不能在 IT 空缺的情况下制定。由于用户的需求各种各样，IT 必须确保制定政策时全部顾及到。

BYOD 政策没有对错，但需要考虑下列问题：

- **设备：** 支持哪些移动设备？仅某些设备还是员工希望使用的所有设备?
- **数据计划：** 组织是否会支付数据计划费用？您发放定期津贴还是员工提交费用报告?
- **合规性：** 哪些规定规管组织需要保护的数据？举例来说，健康保险携带和责任法案 (HIPAA) 要求根据该法案对存放数据的设备进行本机/加密处理。
- **安全性：** 需要实施哪些安全措施（密码保护、破解/获得根权限的设备、防恶意软件应用程序、加密、设备限制、iCloud 备份）?
- **应用程序：** 禁止使用哪些应用程序？IP 扫描、数据共享、Dropbox?
- **协议：** 针对具有公司数据的员工设备，是否有可接受的使用协议 (AUA)?
- **服务：** 员工可以访问哪些资源 – 电子邮件？某些无线网络还是 VPN？CRM?
- **隐私：** 会从员工的设备中收集哪些数据？绝对不会收集哪种个人数据?

就 BYOD 而言，没有问题是禁忌话题。组织必须与员工进行开诚布公的对话，了解他们将如何使用设备， 同时让他们了解 IT 实际中如何满足这些需求。

2. 找出访问公司资源的设备

想象一下：您开始使用 MDM 解决方案时，假设公司支持 100 台左右的设备。您保留了一份详尽的电子表格，记录设备类型和用户 — 这样应该不会有什么意外了。然而，当您第一次去查看报告时，竟然出现有 200 多台设备。这种情形确实存在，并非虚构。且发生的频率比您想象的要高得多。

请勿否认现实。眼不见，并不意味着心不烦。请先了解移动设备使用群体的现况，然后再制定不容更改的战略。为此，您需要一种工具，这种工具需要能够不断与您的电子邮件环境通信，并且能够检测到接入企业网络的所有设备。请记住，一旦为邮箱启用 ActiveSync，即便没有 IT 知识也能毫无障碍地同步多台设备。

所有移动设备都要纳入移动计划中，同时通知设备所有者：公司要落实新的安全政策。

3. 注册应该简单

复杂性容易带来不合规性。一旦确定要注册的设备，您的 BYOD 项目就应该采取相关技术，让用户以简单的方式几步完成注册。这个过程应该简单而安全，同时可对设备进行配置。

理想情况下，用户应该能够按照电子邮件链接或文本，跳转到在设备上创建的 MDM 配置文件 – 包括接受一直重要的 AUA。

将 BYOD 的接入看作一场婚姻，而 AUA 就是支持锦绣良缘的婚前协议。

操作说明应有助于现有用户注册 BYOD 项目。建议现有用户清除其 ActiveSync 帐户，这样您便可以隔离和管理设备上的企业数据。新设备应该首先接受全新的配置文件。

从 IT 角度来看，您希望能够批量注册现有设备，或者让用户自行注册他们的设备。您还需要通过基本的验证流程（例如一次性密码或使用 Active Directory/LDAP 等现有公司目录）对员工进行验证。如有任何新设备试图访问公司资源，应进行隔离并通知 IT。这为 IT 部门提供了灵活性，让他们可以根据批准情况禁止或启动适当的注册工作流程，从而有助于确保公司政策的遵循。

4. 远程配置设备

如果有一件事是 BYOD 政策和 MDM 解决方案不应该做的，那就是把更多用户推向帮助台。您的设备应进行远程配置，从而优化 IT 和业务用户等人员的效率。

用户接受 AUA 后，平台应该提供员工访问所需的所有配置文件、凭据和设置，其中包括：

- 电子邮件、联系人和日历
- VPN 和 Wi-Fi
- 公司文档和内容
- 内部和公共应用程序

此时，您还要制定相关策略，限制某些应用程序的访问权，并在用户超出数据使用范围或者当月津贴限额时生成警告。

5. 帮助用户自助

您会感谢自己做的这一切。用户希望可以正常使用设备，您希望缩短帮助台时间。强大的自助平台让用户可以直接执行下列操作：

- 员工忘记当前密码时进行 PIN 和密码重置
- 使用映射集成通过门户网站直接对丢失的设备进行地理地位
- 远程擦除设备，移除敏感的公司数据

安全、公司数据保护及合规性是大家共同的职责。对员工来说，这可能是难以下咽的苦药，但是如果没有他们的配合，就无法降低风险。自助服务门户可以帮助员工了解他们不合规的原因。

6. 个人信息保密

当然，BYOD 政策并不只是保护企业数据；精心设计的 BYOD 计划还要确保不会将员工个人数据泄露给其他人，包括 IT。个人身份识别信息 (PII) 可用于识别、联系或找到一个人。有些隐私法甚至禁止公司查看此类数据。向员工传达隐私政策，并清楚表明您不会从他们的移动设备上收集哪些数据。举例来说，MDM 解决方案应该能够解析哪些信息可以访问，哪些不能访问，例如：

- 个人电子邮件、联系人和日历
- 应用程序数据和文本消息
- 通话记录和语音邮件

另一方面，让用户知道您收集哪些信息，如何使用这些信息以及这为何会使他们从中受益。

先进的 MDM 解决方案可以将隐私政策转化为隐私设置，进而隐藏设备上的位置和软件信息。这有助于公司遵守 PII 法规，并通过阻止查看智能手机和平板电脑上的个人信息增加员工的舒适度。例如：

- 禁用应用程序库存报告，以限制管理员查看个人应用程序。
- 取消激活位置服务，防止访问位置指标，例如物理地址、地理坐标、IP 地址以及 Wi-Fi SSID。
- 透明和清晰是重要的要求。如果所有人都了解规则，实施 BYOD 政策的阻力就会大大降低。

7. 将个人信息与公司数据分开

BYOD 如同 IT 与用户都赞成的一项协议，个人信息就像生日聚会的照片或是伟大的美国小说，应与生产力应用程序分离开。

简单地说，当员工决定离职时，公司 IT 必须保护公司的应用程序、文档和其他资料，但不得触碰员工个人的电子邮件、应用程序和照片。

这种方法带来了自由度，不仅得到用户的欣赏，IT 也拍手称快，这有可能让他们的生活轻松很多。当有员工离职时，IT 可以通过这种方法，有选择地擦除企业数据。如果员工丢失了设备，IT 可以根据情况，擦除整个设备。真正的 MDM 解决方案可以给您这样的选择。

据估计，大约 86% 的设备擦除是经过精心选择的；仅擦除企业数据。

8. 管理数据使用情况

BYOD 政策很大程度上将 IT 从通信业务中解放出来，但许多公司仍然需要帮助员工管理其数据使用情况，以避免产生过多的费用。

如果您要为数据计划付费，则可能需要采用一种方法来跟踪这些数据。如果您不需要付费，则可能需要帮助用户跟踪他们当前的数据使用情况。您应该能够跟踪设备上网内和漫游数据的使用情况，并且在用户超过数据使用阈值时生成警报。

您可以设置漫游和网内兆数限制，并自定义结算日以基于使用比例生成通知。建议您将使用 Wi-Fi（如可用）的好处告知用户。自动的 Wi-Fi 配置有助于确保设备在企业范围内自动连接到 Wi-Fi。

如果津贴计划每月仅提供 50 美元或仅支付 200 MB 数据的使用费，则员工会在即将超出规定范围时收到一条警告，告知他们要自行负责超出部分。

9. 持续监控设备防止出现不合规

设备一旦注册，便与它所处的环境息息相关。在某些情况下应对设备进行不间断的监控，同时落实自动化策略。用户是否想禁用管理？该设备是否遵守安全策略？您是否需要依据所看到的数据进行调整？从现在起，您将开始了解要制定的其他政策或规则。下面是几个常见问题：

- **从根本上解决破解问题：**为了免费获得付费应用程序，员工有时会对手机执行“破解”或“获取根权限”操作，从而为偷盗信息的恶意软件打开了大门。如果设备已被破解，则 MDM 解决方案应能够采取行动，如立即有选择性地擦除设备上的企业数据。
- **酌情处理；发送短信：**如果是《愤怒的小鸟》之类消耗时间的程序触碰到公司政策，但并不是违反，自动擦除操作就过于严厉了。MDM 解决方案可以根据违反程度执行政策。MDM 可以向用户发送信息，规定时间删除应用程序，如不执行，再由 IT 擦除。
- **新增可用操作系统。**要想 BYOD 一直有效，用户需要一个简单的方法来提醒他们有新的操作系统可以安装。借助合适的 MDM 解决方案，操作系统升级就成了一项自助功能。限制过时的操作系统版本有助于确保合规性和优化设备的可操作性。

10. 坐享 BYOD 带来的投资回报 (ROI)

BYOD 将购买设备的责任转移给了员工，这种情况下，花时间考虑企业的宏图蓝图和长期成本是值得的。

制定政策时，您应考虑该政策会对 ROI 产生怎样的影响。这包括如下文所示那样对不同方法进行比较：

公司所有模式

- 每台设备要花费多少成本
- 全额补贴的数据计划成本
- 每隔几年回收设备的成本
- 保修计划
- 管理项目所需要的 IT 时间和劳动力

BYOD

- 部分补贴的数据计划成本
- 设备采购的预计成本
- 移动管理平台的成本

一劳永逸的办法并不存在，但精心拟定的 BYOD 政策会为您高效管理移动设备指明方向。

当然了，当员工经常移动且时刻接入时，通常才会看到生产力提高。BYOD 是种不错的方法，让以前可能没有资格享用公司设备的新用户也能提高生产力。

BYOD：自由的安全性

BYOD 是一种新兴的最佳实践，赋予员工在自己的设备上工作的自由度，同时减轻 IT 繁重的财务和管理负担。但是，如果没有精心制定的政策和强大的管理平台，BYOD 就无法兑现简化管理并节省成本的承诺。

如果您仍处在移动战略的早期阶段，IBM® MaaS360® 会为您提供丰富的培训资源。

如果您认为 BYOD 就是企业的最佳选择，请单击此处，免费试用 MaaS360 30 天。由于 MaaS360 是基于云的方案，您的测试环境会自动变成生产环境，不会丢失任何数据。

IBM MaaS360 简介

IBM MaaS360 是一款企业级移动性管理平台，让人们的工作方式更高效，同时实现数据保护。数以千计的组织信赖 MaaS360，将它作为实施移动性计划的基础。MaaS360 可为用户、设备、应用程序和内容提供具有强大安全控制的全面管理，从而支持所有移动部署。如需了解有关 IBM MaaS360 的更多信息，并开始 30 天的免费试用，请访问：www.ibm.com/maas360

IBM Security 简介

IBM 的安全平台提供安全资讯，帮助组织为员工、数据、应用程序和基础架构提供全方位保护。IBM 提供下列解决方案：身份和访问管理、安全信息和事件管理、数据库安全、应用程序开发、风险管理、端点管理、新一代入侵防御等。IBM 是全球最广泛的安全研发和交付组织之一。如需更多信息，请访问 www.ibm.com/security

IBM CorporationS
oftware Group
Route 100
Somers, NY 10589

美国印制 2016 年 3 月

WGW03112-CNZH-01