BYOD 的十大戒律

MaaS360
by Fiberlink

MaaS360® by Fiberlink, an IBM company

您应支持BYOD

随着移动设备在工作场所内的快速普及，许多IT领导者感觉自己犹如神助。冥冥中好像有个声音让您支持的所有员工使用尽可能多的设备并让这些设备互连，使公司服务实现一体化。自带设备(BYOD)趋势已形成，员工们也都热情地表示支持。

阻挡此趋势发生或者执意坚持不允许自己的员工这样做都没有任何意义。事实是，员工们已经在这样做并且会继续将不符合要求的设备连接到您的网络，而不管您是否允许。Forrester对美国信息工作者的研究表明，在正式权限和政策确立之前，有37%的员工在工作中使用相关技术产品。[1] 另外，Gartner CIO的一项调查确定，到2016年将有80%的员工有资格使用自己的设备，并且可以在设备上存储员工数据。[2]

这样就提出了一个不可避免的问题：您该如何满足员工使用个人应用程序和设备的愿望，同时允许他们在保护公司数据的安全环境下高效工作？BYOD的十大戒律将向您介绍如何创建稳定、安全且高效的移动环境。

BYOD的十大戒律

1. 引进技术之前先制定政策
2. 替员工的设备摸底
3. 注册流程应简单明了
4. 您应以无线方式配置设备
5. 您的用户要求自助服务
6. 保护个人私密信息
7. 划分公司数据和个人数据
8. 自动监控员工设备使用情况
9. 管理您的数据使用量
10. 通过改善ROI获利

[1] 本杰明·格雷(Benjamin Gray)和克里斯蒂安·凯恩(Christian Kane)，“十五项移动策略最佳做法”(Fifteen Mobile Policy Best Practices)，Forrester研究，2011年1月。

[2] 肯·杜兰尼(Ken Dulaney)和保罗·德比艾斯(Paul DeBeasi)，“管理企业员工拥有的技术”(Managing Employee-Owned Technology in the Enterprise)，Gartner Group，2011年10月。

MaaS360® by Fiberlink, an IBM company

1. 引进技术之前先制定政策

如同其他任何IT项目，政策必须先于技术，即使是云技术也是如此。要使员工自有设备有效利用移动设备管理(MDM)技术，您仍然需要制定相关政策。这些政策不仅会影响IT，还会影响HR、法律和安全部门，即以生产效率的名义使用移动设备的任何企业部门。

由于BYOD政策会影响所有业务范围，因此不能只关乎IT方面。用户需求多种多样，IT必须确保制定政策时考虑了所有这些方面。

暂时没有泛用的BYOD政策，但制定正确政策需要考虑下面的一些问题：

- **设备**：哪些移动设备受支持？仅部分设备，还是员工需要的任何设备？

根据Forrester的调查，70%的智能手机为用户所有，12%购自核准的商家，而16%则由公司提供。65%的平板电脑为用户所有，15%购自核准的商家，而16%则由公司提供。换句话说，大部分用户使用的是自己的设备。

- **数据流量**：企业是否承担产生的数据流量费？您会发放津贴，还是由员工提交费用报告？

谁支付这些设备的费用？对于智能手机，70%支付全款，12%获得折扣，3%支付部分金额，而剩余的15%则由公司支付全款。对于平板电脑，58%为用户自己购买，17%获得公司折扣，7%分摊费用，而18%则由用户公司发布并付款。（来源：Forrester，2011）

- **合规性**：哪些法规管辖您的企业需要保护的数据？例如，《健康保险携带和责任法案》(HIPAA)要求公司对所有存储受该法案约束的数据的设备进行本机加密。
- **安全性**：需要采取哪些安全措施（密码保护、破解/初始化设备、反恶意软件设备、加密、设备限制、iCloud备份）？
- **应用程序**：哪些应用程序被禁止使用？IP扫描、数据共享、Dropbox？
- **协议**：针对存储有公司数据的员工设备，有没有可接受使用协议(AUA)？
- **服务**：员工可以访问哪些类型的资源—电子邮件？某些无线网络或VPN？CRM？
- **隐私权**：可以从员工设备收集哪些数据？绝对不能收集哪些个人数据？

考虑BYOD问题不应当有所避讳。关于如何使用设备以及IT如何实事求是地满足这些需求，需要进行坦诚布公的对话。

MaaS360® by Fiberlink, an IBM company

2. 替员工的设备摸底

请想象一下。在假设您的公司支持100台左右的设备的前提下，您开始使用MDM解决方案。您已将设备类型和用户制成精确的电子表格，这点没什么可惊奇的。但是，当您首次查看报告时，却有200多台设备显示。这是事实，并非虚构。这种情形的发生频率超出您的想象。

请不要否认事实。您所不了解的方面可能会给您带来伤害。确定自己的策略之前，请先了解下当前使用移动设备的人数。为此，您需要一个能与您的电子邮件环境实时通信，并能检测连到您公司网的所有设备的工具。请注意，为邮箱启用ActiveSync之后，即使您不懂IT知识，通常也可以毫无障碍地同步多台设备。

所有移动设备均需纳入您的移动报告，并且如果新安全政策付诸实施，则需要通知各设备的所有者。

3. 注册流程应简单明了

导致违规的最大原因就是流程过于复杂。您确定要注册的设备之后，您的BYOD项目应该利用支持低接触的简单用户注册方式的技术。流程应简单、安全，并在同一时间配置设备。

理想情况下，用户应该能够通过电子邮件链接或文本找到针对自己设备创建的MDM配置文件（包括接受越来越重要的AUA）。

> 如果将使用BYOD视作一场婚姻，那AUA就可以算是确保和谐关系的婚前协议。

相关说明应该可以帮助现有用户注册BYOD项目。我们强烈建议现有用户清除现有的ActiveSync帐户，以便分门别类地管理设备上的公司数据。新设备应该具有全新的配置文件。

从IT角度来看，您需要能够批量注册现有设备，或者让用户自行注册各自的设备。您还需要根据基本的验证流程（例如，一次性密码或使用现有的公司目录，像Active Directory/LDAP），对员工进行验证。任何尝试访问公司资源的新设备都必须分离出来并且通知IT。这样一来，如果获得批准，IT可以灵活地阻止或启动合适的注册流程，确保遵循公司政策。

MaaS360® by Fiberlink, an IBM company

4. 您应以无线方式配置设备

如果存在BYOD政策和MDM解决方案均无法解决的问题，则会有更多用户访问帮助台。您应以无线方式配置所有设备，以便IT和企业用户均实现最大效率。

用户接受AUA之后，您的平台应该提交员工需要访问的所有配置文件、凭据和设置，其中包括：

- 电子邮件、通讯录和日历
- VPN
- 公司文档和内容
- 内部和公共应用程序

此时，您还应创建用于限制某些应用程序的访问权限的相关政策，并且在用户超出本月数据使用量或津贴限制时生成警告。

5. 提供用户自助服务

您会为自己所做的一切感到欣慰。用户需要正常运行的设备，而您需要优化帮助平台的时间。强大的自助服务平台允许用户直接执行以下操作：

- 员工如果忘记当前的PIN码和密码，可以重置一下
- 使用映射集成，通过门户网站对丢失的设备进行地理位置定位
- 远程擦除设备，清除所有敏感的公司数据

安全性、公司数据保护以及合规性是大家共同的责任。员工可能难以独自承担以上责任，但是如果没有员工的合作，根本无法降低风险。通过自助服务平台，员工可以了解自己为何可能不符合要求。

MaaS360® by Fiberlink, an IBM company

6. 保护个人私密信息

当然，BYOD政策不仅会保护公司数据；BYOD项目经过精心设计，可以确保员工数据私密、安全。个人验证信息(PII)可用于识别、联系或找到相关人员。部分隐私法禁止公司查看此类数据。向员工讲述隐私权政策，使其清楚您不能从他们的移动设备中收集哪些数据。例如，MDM解决方案应该能够解析它可以和不可以访问的信息，例如：

- 个人电子邮件、通讯录和日历
- 应用程序数据和文字消息
- 通话记录和语音邮件

另一方面，让用户了解您可以收集的信息及其使用方式，以及用户为何能从中受益。

高级MDM解决方案可以将隐私权政策转变为隐私权设置，以隐藏设备上的位置和软件信息。通过阻止查看智能手机和平板电脑上的个人信息，这样有助于公司满足PII法规，并且让员工更加放心。例如：

- 停用应用程序清单报告可以限制管理员查看个人应用程序
- 停用定位服务可以阻止访问位置指标，例如物理地址、地理坐标、IP地址和WiFi SSID

透明度和清晰度是重要的标语。当所有人都了解相关规则时，BYOD政策受到的阻力会大大减少。

7. 划分公司数据和个人数据

要让BYOD成为IT和最终用户共同遵守的协议，个人信息（例如生日聚会照片或著名的美国小说）应与生产型应用程序分离。

简单地说，如果员工决定离开公司，则公司IT必须保护好公司应用程序、文档和其他材料，但不得查看个人电子邮件、应用程序和照片。

不仅用户欣赏该方法所体现的自由性，IT也很欣赏，因为他们的生活为此变得无限轻松。借助此方法，IT可以在员工离开公司时选择性地擦除公司数据。根据具体情况，如果员工丢失设备，则可以擦除设备上的全部数据。但是，只有真正的MDM解决方案允许您这样做。

86%的设备擦除是选择性的；只有公司数据会被擦除。

MaaS360® by Fiberlink, an IBM company

8.自动监控员工设备使用情况

设备注册之后，一切取决于具体环境。在某些情形下，应该不断监控相关设备，并且确保实施自动化政策。用户是否尝试停用管理？设备是否符合安全政策？您是否需要根据自己查看的数据进行相应调整？从目前开始，您可以开始了解要创建的任何额外政策或规则。下面列出了一些常见的问题：

- **获取破解“根源”**：为免费获得付费应用程序，员工有时会“破解”或“初始化”手机，从而让可窃取信息的恶意软件有了可乘之机。如果某设备遭破解，MDM解决方案应该能采取相关措施，例如立即从该设备上选择性清除公司数据。
- **选择性擦除；发送SMS**：如果时间杀手（例如Angry Birds）与企业政策相冲突但没有进行攻击，则立即清除可能有些严重。MDM解决方案可以根据攻击行为强制执行相关政策。MDM可以通知用户，并且在IT点击“擦除”按钮限期之前提供清除应用程序所剩余的时间。
- **新的可用操作系统**。要让BYOD持续有效，需要有一种简单的方式让用户能在新操作系统准备好安装时获得提醒。借助合适的MDM解决方案，操作系统升级成为自助服务功能。限制过时的操作系统版本可确保合规性并最大限度地提高设备的可操作性。

9. 管理您的数据使用量

BYOD政策很大程度上让IT免于通信业务，但大部分公司仍然需要帮助员工管理各自的数据使用量，避免产生过高费用。

如果您要承担数据流量费，则可能需要采用一种方法来跟踪此类数据。如果您不用承担这种费用，则可能需要帮助用户跟踪他们当前的数据使用量。您应该能跟踪设备上的网络和漫游数据使用量，并且在用户超出数据使用量阈值时生成警告。

您可以设置漫游和网络兆位限制并自定义结算日，以根据所用百分比创建通知。我们还建议向用户讲述使用WiFi（如果可用）的好处。WiFi自动配置有助于确保设备处于企业位置时自动连接到WiFi。

如果津贴计划每月仅覆盖50美元或200 MB的数据使用量，则员工可能会收到超支警告。

MaaS360® by Fiberlink, an IBM company

10. 通过改善ROI获利

BYOD将购买设备的责任转移给了员工，就公司大局和长期成本而言，这是值得的。

制定政策时，您需要考虑一下该政策将如何影响ROI。其中包括对方法进行比较，如下表所示：

公司经营模式	BYOD：
每台设备所需的费用	部分资助的数据流量费
全数资助的数据流量费	免除购买设备的成本
每隔几年回收设备的成本	移动管理平台的成本
保养维修计划	
IT在管理项目方面所耗费的时间和精力	

没有放之四海而皆准的政策，但是BYOD政策经过精心设计，可以提供相关指导，这是您有效且高效地管理移动设备所必需的。

当然，如果员工可以自由流动并且随时联系在一起，则生产效率会有所提高，这已是司空见惯的事情。借助BYOD这一伟大方式，让之前可能没有资格使用公司设备的新用户提高了生产效率。

BYOD：自由中实现安全

BYOD是新兴的最佳做法，允许员工自由使用自己的设备工作，同时让IT免于沉重的财务和管理负担，但如果没有良好的政策和强大的管理平台，BYOD肯定不能实现简化管理且节约成本的目标。

如果您确定BYOD适合自己的业务，请点击此处开始免费使用MaaS360三天。由于MaaS360基于云，因此您的测试环境会立即成为开发环境，但不会丢失任何数据。

如果您仍处于移动策略的初级阶段，则MaaS360会提供丰富的教育资源，如下所示：

www.maas360.com
http://www.maas360.com/products/mobile-device-management/
MaaSters Center

了解详情
要详细了解我们的技术和服务，请访问www.maaS360.com。
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
电话 215.664.1600 | 传真 215.664.1601 | sales@fiberlink.com