BUILDING AN EFFECTIVE MOBILE POLICY

A comprehensive policy for devices, applications and content helps organizations get the most out of mobile technologies.

Executive Summary

A growing number of organizations are realizing the benefits of mobile devices, including increased productivity, enhanced efficiency and speedier response times. Yet while the use of mobile devices typically leads to lower costs and additional revenue opportunities, it also brings challenges associated with device and application procurement, data connections, service costs, content management and — most important — security.

As the number of workers who use smartphones, tablets and notebooks on the job skyrockets, it’s no longer sufficient to rely on casual or ad hoc policies for mobile devices. A formal mobile policy is essential to derive the maximum benefit from the use of these devices and to avoid the common oversights and mistakes that can lead to potentially devastating consequences.

When an organization begins defining its mobile policy, it must address the various technologies and processes that form the foundation of a comprehensive mobility program, including devices, management, security, applications and services. Organizations also need to establish their mobile program’s focus, scope and goals.

According to a Cisco Systems study, 51 percent of U.S. businesses already have an organizational mobility strategy. Most of the other 49 percent either are currently working on a mobility program or soon will be. With forethought and organizationwide goals in mind, IT decision-makers can create a policy that satisfies both organizational and employee needs, protects data and creates low management overhead.

Table of Contents

1 Executive Summary
2 The Need for an Effective Mobile Policy
3 Mobile Devices: BYOD Versus COPE
3 Security
5 Management
5 Applications
6 Mobility Services
8 CDW: A Mobility Partner That Gets IT
The Need for an Effective Mobile Policy

Organizations worldwide are embracing mobile technology because it offers a competitive advantage. By enhancing productivity and efficiency, mobile devices transform the way users approach work and accomplish tasks.

According to a survey conducted by Enterprise Mobility Exchange, an online community for global mobility professionals, the main drivers behind planned mobility solution investments include:

- Increasing productivity: 68%
- Improving operational efficiency: 50%
- Boosting profitability: 38%
- Improving customer service: 36%
- Reducing costs: 30%
- Remaining competitive: 29%
- Streamlining operations: 25%
- Generating additional revenue: 14%
- Reducing project timelines: 13%

Applications: The mobile policy should specify the required applications for specific tasks as well as who should supply the application (the organization or the user). The policy should also specify how and when applications are to be upgraded. According to a survey of 160 IT professionals conducted by the Spiceworks online community, the most common types of applications that organizations allow mobile devices to access are web apps (84 percent), intranet apps (61 percent) and extranet partner apps (40 percent).

Access to organizational data: The mobile policy should clearly specify which employees are allowed to access which types of data, from where and using what kinds of devices. As long as established security procedures are followed, mobile device data access rights can safely mirror office desktop computer clearance levels. According to the Spiceworks survey, most organizations (84 percent) now allow mobile users to access their systems via an on-premises local area network.

Mandatory security controls: The policy should outline the minimum mandatory security measures (such as encryption, PIN codes or remote wiping) that must be implemented on each mobile device in the organization. An organization may decide to disallow some types of inherently unsecure devices from accessing internal networks.

Financial terms: There are three basic approaches to funding a mobile device program: direct billing, in which the organization buys the device and assumes all expenses; fixed monthly reimbursement for device support; and reimbursement based on staff expense reports. A growing number of organizations are using their existing travel and expense reporting systems to manage mobile expenses. IT leaders should communicate the approach being used in the mobile policy.

Liability and ramifications: The mobile policy should include security, privacy and other guidelines that will help limit potential liability if information is lost or stolen via a mobile device. Particularly important are stipulations that affect how users obtain, utilize and communicate information on their devices. Mobile device liability is a complex and rapidly evolving area of law. This part of the mobile policy should be developed in close consultation with an attorney.

Penalties for noncompliance: A mobile policy usually includes several levels of noncompliance penalties. The policy should specify simple reprimands for users who fail to follow a particular use or security rule, or who engage in excessive use of mobile services over an extended period of time after being warned by a supervisor. Fines and restitution may be imposed on users who employ organization-owned devices to purchase nonessential or personal services. Employment termination may even be specified for a user who fails to promptly report a lost or stolen device that contains customer or employee information. Downloading software or content that is obscene, offensive or in violation of the organization’s tolerance policy, particularly to an organization-owned device, may also be specified as a cause for dismissal.

Mobility is a powerful resource that should never be approached on an ad hoc or piecemeal basis. Simply allowing users to employ any type of mobile device, for whatever purpose they choose, opens the door to poor performance, wasteful spending, security vulnerabilities and other serious concerns. Every organization that utilizes mobile devices should have a comprehensive, formal written mobile policy document. The essential elements of a mobile policy include the following:

Device specification: The mobile security policy should define which types of mobile devices are permitted to access the organization’s resources and the degree of access for the various classes of mobile devices (such as organization-issued devices versus personal devices).

Device use and access: Users need to know when and where it is appropriate to use a mobile device and which type of device (smartphone, tablet or notebook) to use in specific situations.
Mobile Devices: BYOD Versus COPE

Organizations that are adopting various types of smartphones, tablets and notebooks must decide how these devices will be provided to users, paid for, managed and supported. While users will bring their own mobile gadgets to work no matter what, organizations may prefer to issue their own devices, for example, when an important app requires a specific type of mobile platform.

Any smartphone, tablet or notebook used in the workplace fits into one of two models: bring your own device (BYOD) or corporate-owned, personally enabled (COPE).

A BYOD strategy permits users to work with a personally selected and purchased mobile device to run work-related applications and access data. BYOD allows users to select the devices that best meet both their personal and their work needs. An organization’s IT department typically supplies data access, technical support and security services. In some cases, users are partially or fully compensated for their device purchases. According to an April 2015 Pew Research survey, 64 percent of U.S. adults now own a smartphone, up from 58 percent in early 2014. Many of these people would prefer to use their own phones while at work, helping to strengthen the BYOD trend.

COPE flips the BYOD model on its head. COPE requires users to work with smartphones, tablets and notebooks issued by their employer instead of using their own devices. The policy isn’t as restrictive as it sounds: With COPE, users can generally employ their work devices for personal tasks too. In most cases, workers can post, text and tweet to their hearts’ content as long as their activities don’t contravene organization policies or interfere with work responsibilities.

While BYOD still has its proponents, COPE might be gaining steam as a mobile device workplace model. From an employer’s perspective, BYOD creates new burdens by demanding support for a seemingly infinite array of platforms and profiles. COPE, on the other hand, allows and supports both business and personal use of an organization’s devices while limiting the types of devices that IT staff members must deal with.

According to the Aberdeen Group, factors such as recent court rulings and increasing user unwillingness to surrender any control over their own devices are reducing BYOD’s overall appeal. IT departments are discovering that while BYOD can save on initial hardware costs, the lost security, management and control capabilities may not be worth the savings.

A mobile policy should specify the type and level of support the organization will offer device users in areas such as connection fees, accessories, repairs, training, app delivery and updates. If organizational data on a mobile device must be separated from the user’s personal data, the mobile policy should define such requirements, including storage partitioning. Users must be trained in how to ensure that information is stored in the work data partition instead of on the personal side, such as when taking notes in a sensitive meeting or documenting the contents of a whiteboard with the device’s camera.

If a BYOD program has been implemented, the policy should also specify exactly which types of mobile devices employees are allowed to use on the job. For reasons such as app availability or device management conformity, an organization might decide to create an Android- or iOS-only policy. The mobile policy might also require a BYOD device to use a specific OS release. In the case of iOS devices, an organization will likely want to ban “jailbroken” devices due to the potential security risks they pose.

Security

Security must be an integral part of every organization’s mobile policy. According to a December 2014 survey from Forrester Research, more than 64 percent of IT decision-makers said they expected their mobile security budgets to increase in the next 12 months.

The core security components for mobile deployments include mobile device management (MDM), mobile application management (MAM) and mobile content management (MCM). Several mobility vendors have integrated these tools into Enterprise Mobility Management (EMM) solutions that help organizations realize the rewards of a mobile deployment while mitigating the risks of a
diverse mobile environment. All these tools are available via in-house software, cloud-based services or hybrid solutions.

**MDM:** These solutions are essential for enforcing mobile policies because they allow an organization to continuously monitor, organize and secure employee mobile devices based on different operating systems, and they can be deployed across various mobile service providers. Approximately half of the organizations Forrester surveyed have already adopted MDM technologies.

**MAM:** With the skyrocketing number of mobile applications, deploying, tracking and supervising apps on employee devices has become a major challenge. MAM tools ensure the secure installation and administration of apps on end users’ devices. MAM tools also automate and track app configurations, licensing requirements, updates and use. Many MAM tools can also match mobile device models, usage and ownership to mobile policy requirements.

**MCM:** Giving mobile users fast, easy and reliable access to data without sacrificing security is one of the trickiest tasks facing mobile adopters and IT departments. MCM tools help organizations foster employee collaboration and productivity by establishing secure content access and sharing across devices — whether the content is located on the organization’s network or in the cloud.

IT decision-makers should also look for security tools that offer robust features for managing and protecting mobile devices. There are several key features that organizations should consider when choosing these tools.

**Remote management and wiping:** IT administrators should be able to remotely monitor and manage mobile devices to ensure that users are following the organization’s policies. Should a device be lost or stolen, the ability to remotely wipe it can prevent data from falling into the wrong hands. Many vendors offer containerization features that allow administrators to wipe an organization’s data while leaving personal information intact.

**Data loss prevention and encryption:** Data is the most valuable asset contained on any mobile device, and any breach of data security can result in a crisis. Data loss prevention tools allow IT departments to set policies regarding how data is moved and used. Encryption scrambles the data on a device and requires a key for unscrambling, which reduces the chance that unauthorized users may gain access to an organization’s sensitive data.

**Network security:** The network is a focal point of any security effort. Solutions such as firewalls, virtual private networks, intrusion prevention systems and application controls provide a variety of defensive capabilities. Advanced tools such as next-generation firewalls can deliver even greater levels of security as well as management control.

**Client virtualization:** Solutions that move computing and data storage functions to a central data center, which serves out data and applications to remote devices, can greatly improve security posture.

**Integrated end–to–end security:** Some vendors offer solutions that combine numerous security capabilities, which can increase the protection they offer.

---

### THREE PILLARS OF MOBILE DEVICE SECURITY

Mobile devices are moving targets. They often roam far beyond an organization’s onsite security perimeter — outside of the protection ordinarily afforded by network firewalls, threat management controls, spam and content filtering, and the various other tools and techniques that are routinely used to ward off attackers. Here are three proven tactics for maintaining control over mobile devices:

1. **Lock down the devices.** A growing number of mobile devices now offer enhanced access controls, such as fingerprint readers, extended passcodes and dual-authentication systems. Such technologies make it more difficult for unauthorized individuals to access an organization’s data on lost or stolen devices. According to market research firm Tractica, mobile device fingerprint readers alone will surpass 1 billion units annually by 2021.

2. **Perform periodic security audits and penetration testing.** Many organizations use a security-testing partner to annually or semi-annually audit their mobile security policies and practices. Such firms can also help resolve any security issues that an audit discovers and prepare for new threats.

3. **Control third–party apps and files.** Organizations that issue mobile devices to employees should have policies that either restrict or block third–party apps and file downloads. This practice will prevent security breaches created by the unintentional installation of rogue software incorporating backdoors and other data-stealing methods. According to a survey of IT professionals conducted by the Spiceworks online community, the attack vectors of greatest concern to organizations managing mobile devices include malicious file downloads (57 percent of respondents), malicious apps (50 percent) and email (48 percent).
Management
Mobile device management would be far easier if a simple all-encompassing policy met the needs of all organizations. Yet a blanket management policy is impossible because each organization has unique needs and uses its mobile devices in different ways. To cover all key mobile device management considerations, organizations must address a variety of issues.

Liability
Mobile devices create two potential areas of liability: data security and user behavior. Data security practices must be adopted that accommodate the organization’s regulatory environment and risk tolerance.

On the user side of the coin, organizations are likely liable for actions a user performs on the job with his or her mobile device, but they are not usually liable for a device the user owns and brings to work. Users are, however, generally personally liable for the early termination fees associated with their personal mobile devices and service plans if they choose to discontinue the service prior to the conclusion of the contract.

Privacy
It’s important to fully inform all mobile device users exactly how, when and where they can use their devices. IT staff must ensure that all BYOD users understand the implications of connecting their personal devices to the organization’s network. On organization-supplied devices, the use of lockdown functions on smartphones and tablets can prevent users from accessing forbidden features.

It’s also essential to inform users about the exact tracking and monitoring tasks the organization may perform. A mobile policy document, for example, may state that location tracking will be used only if a device is lost or stolen. However, an organization is well within its rights to monitor a user’s mobile activities while the device is connected to the network.

Financial Responsibility
Users need to know how and when the organization will cover service plans and other costs. IT leaders should create a system to handle and approve mobile device expenditures, including how to submit invoices and expense reports and whether management approval must be obtained before a staff member can apply for reimbursement.

Additionally, mobile expense management software, whether provided by an EMM solution or a stand-alone product or service, enables managers to reconcile carrier invoices to assets, provide custom usage reports and invoices to meet finance or chargeback needs, access critical mobile inventory and expense information, and obtain insights into other key aspects of mobility finance.

Other issues that IT leaders should address in their mobile policies include:

- **Real-time monitoring:** Monitoring software, often integrated into an EMM product, enables an organization to keep an eye on mobile device performance and activity, typically to monitor trends and forecast future requirements. This feature should not be used to spy on users’ nonbusiness actions and behavior, a fact that should be stated in the mobile policy.

- **Custom reporting:** Many EMM solutions and other management tools offer custom reporting features that generate insights into key financial, use or performance aspects of an organization’s mobility infrastructure. Such reports can be used to detect hidden problems, reduce costs or improve mobile device use.

- **Third-party security services:** Security lies at the heart of mobile management. Yet many organizations lack the internal resources to ensure continuous security. Third-party security services fill this critical need, helping protect devices from malware and other threats by ensuring security-rich access to systems and safeguarding data and applications.

Applications
Mobile apps are where the rubber meets the road for mobility deployments. An organization that uses mobile apps effectively can reap significant benefits. Without an effective mobile app policy —
one that covers factors such as app stores and app procurement or development — an organization can soon find itself mired in problems.

Mobile apps are typically delivered to end users via an app store. While iOS-based phones and tablets are restricted to Apple’s proprietary marketplace, users of Google Android and Microsoft Windows mobile devices can download apps from a variety of different sources. A growing number of organizations also are creating their own marketplaces, offering users specific task-related apps that have been pretested for performance, security and safety.

Gartner reports that mobile apps often misbehave without anyone knowing. They may contain exploitable vulnerabilities, violate mobile policies, spy on users or customers, or manipulate a device’s expected functions. IT departments must obtain risk/security reputation ratings for commercial apps and allow app downloads only from trusted developers.

To enhance security and improve employee productivity, many organizations opt to blacklist or whitelist specific apps. Blacklisting prevents the use of potentially dangerous or time-wasting apps by establishing a list of apps that users are not allowed to download. Whitelisting limits device users to a preselected collection of work-related apps. Both whitelists and blacklists are typically created and enforced by IT staff via MAM software.

As they establish mobile policy, organizations must consider carefully whether they will purchase commercial apps off the shelf or develop their own custom applications.

Off-the-shelf apps deliver a wide array of collaboration, office productivity, security and backup services. The drawback to these apps is that they are designed to meet the needs of a broad swath of users and often fail to address a specific organization’s unique needs. However, off-the-shelf apps are generally much less expensive than custom apps and are supported and updated by their developers at little or no extra cost.

Many organizations deploy custom mobile apps designed to meet a unique need or streamline an essential task, such as inventory management, deliveries or customer service. The downside is that custom-designed apps are expensive and may require a significant period of time to develop and test. A faster, less expensive alternative is the deployment of applications with customizable user interfaces that can be adapted to meet specific needs of an organization and its users.

Client virtualization offers an alternative to custom mobile apps. Client virtualization technologies allow organizations to deploy both apps and desktops securely and efficiently to almost any device over nearly any network. With app virtualization — the most common client virtualization approach — apps are virtualized into executable files that are run directly from the client device. Applications can then function securely, and completely isolated from each other as well as from the operating system, leading to conflict-free execution on various mobile devices.

With desktop virtualization, the operating system and applications are stored inside a data center and are streamed to the user via any desktop or mobile device. Desktop virtualization users have the freedom to connect to the organization’s network at any time from any location on virtually any device. Desktop virtualization allows greater control over the IT environment, enhancing security and compliance while making processes far more consistent and streamlined. This facilitates deploying new applications and patches, conducting training and repair, and maintaining hardware.

**Mobility Services**

A trusted partner can deliver services that smooth the deployment of a mobility program, from planning through device replacement. As an organization establishes its mobile policy, it should carefully consider these services.
**Help desk services:** Organizations that have already deployed an IT help desk, or have contracted with a help desk service provider, should consider expanding the help desk’s scope to include mobile device support. However, solid user training can help reduce the number of help desk calls related to mobility issues. Gartner recommends a one-hour class during which a user enrolls his or her device and learns how everything works.

**Self-service portal:** Mobile devices are complex, often finicky gadgets. User questions about them can drain IT staff resources. Creating a web-based self-service portal, either internally or with the assistance of a support service provider, can help users quickly and painlessly find solutions to an array of common problems without involving IT staff members.

**Warranties:** For organization-supplied devices, an extended warranty service can help mitigate repair and replacement costs. Device manufacturers, authorized resellers and third-party insurers all offer extended warranty plans. Some partners also offer services to help ensure that organizations are getting maximum value under the terms of their warranties.

**Lifecycle planning:** The lifecycle of an organization-provided device has three stages. At the first stage, provisioning/configuration, the device is loaded with the different apps a user needs and configured to securely bring it onto the mobile and enterprise networks. This is also the stage where all access and permission levels are set and granted to the user and the device. The next step, active life, covers the device’s entire productive life. At this stage, the device must be carefully managed and periodically updated to ensure continued efficient and secure operation. App and operating system updates, device monitoring, asset tracking, device performance assessments, maintenance and reconfiguration processes, and distribution of new and updated data files are some of the major tasks required during this stage. Decommissioning is the final stage in the mobile device’s active life and usually occurs when a device can’t be repaired, is lost or stolen, or is made obsolete by a newer technology. A device may also be decommissioned or, if still in useful condition, returned to the provisioning/configuration stage when its user leaves the organization.

**Device purchases, customization and deployment:** If an organization uses a COPE strategy, users should be able to select from an array of devices (including smartphones, tablets and notebooks) that meet their specific needs. Both COPE and personally owned devices can be configured and customized by an organization to include unique user profiles, time-based profiles, account access requirements, and the installation of work-related applications and content.

**Cross-carrier activations:** Teaming with a mobility services partner that supports cross-carrier activation will enable an organization to activate devices with the carrier of its choice and track expenses and use across each carrier and usage plan.

**Asset tagging and management:** By physically tagging its mobile devices, an organization can optimize device allocation, coordinate lifecycle activities and detect thefts. Data capture services also allow organizations to consolidate all device and network identifiers into a database that can be accessed via a secure website.

**Laser etching:** Using a laser-guided method to imprint identifiable information on a mobile device is an inexpensive and effective way to track and protect valuable assets. If a lost or stolen device is recovered by an honest party, the identification data allows the device to be returned to its owner.

**Burn-in:** A mobile device is most vulnerable to failure (minor or catastrophic) during its first few hours of operation, as various components settle in and begin operating. A mobile partner can quickly examine a new or refurbished mobile device for any obvious faults and then let it run unattended for a few hours before assigning it to a user.

**Procurement portal:** For many organizations, particularly government agencies, procurement portals conveniently consolidate all procurement and provisioning information into a single location. A procurement portal typically provides an automated process that allows users to order from a predefined catalog of mobile devices and accessories, perform upgrades or change existing services — all in accordance with the organization’s mobile policy.

**Device replacement:** Any organization that distributes mobile devices to employees needs to create a policy for replacing defective, lost or stolen units. The policy should clearly define who will bear the financial responsibility for lost or damaged devices. The policy may also specify a penalty for a worker who intentionally damages or destroys a device.

**Mobile accessories:** These accessories include essential items such as chargers, batteries and cables, as well as optional products, such as carrying cases and speakers. The mobile device policy should specify which accessories an organization will pay for and which are the users’ responsibility.

**Managed device subscriptions:** For organizations with limited IT budgets, a managed device subscription is an affordable way to provide smartphones and tablets to users. By purchasing subscriptions that bundle together devices, mobility management software and help desk services, IT departments can easily extend mobility programs to all users and reduce the workload that a mobility program can create for IT staff.

---

88% The percentage of U.S. organizations that issue smartphones to employees instead of using a BYOD strategy

**SOURCE:** Cisco Systems, “Enterprise Mobility Landscape Wave II,” April 2014

lifecycle activities and detect thefts. Data capture services also allow organizations to consolidate all device and network identifiers into a database that can be accessed via a secure website.
CDW: A Mobility Partner That Gets IT

CDW can help organizations of all sizes establish an effective mobile policy that covers mobile devices, apps, accessories and support services — and then help them carry it out with maximum efficiency, productivity and security.

CDW’s team of highly certified IT solutions providers are experts with a wide breadth of knowledge. They listen carefully to each customer to understand the organization’s needs, goals and budget and then provide a clear view of every solution option. CDW works hard to seamlessly align the user experience with business needs. CDW’s account teams — as well as expert presales solution architects, assessment teams and certified engineers — can assist any organization onsite or offsite.

To learn more about addressing vulnerabilities in a mobile environment in which risk is constantly growing, read CDW’s Mobile Security Tech Insights Guide.

Microsoft Surface

Microsoft® offers a substantial lineup of mobility products to meet your organization’s needs — including the Surface™ Pro 3 and the Surface 3. Fold back the keyboard, and you have the ideal hand-held, touch-screen tablet. The USB port lets you connect a wireless mouse or share files with a thumb drive. Its video-out port allows you to connect to an external monitor so you can work like you would on a desktop. Take your pick of thousands of apps in the Windows® app store. While providing great productivity and ease of use for your organization, Microsoft products offer easy, secure integration into your environment.

CDW.com/microsoft