WHITE PAPER

CDW PEOPLE WHO GET IT CANADA

MOBILE POLICY CHECKLIST

Here's what to consider when putting together a mobile policy designed to support a highly productive workforce.

Executive Summary

Since 2010, the use of mobile devices in the workplace has skyrocketed. By 2016, wireless devices will account for 61% of IP traffic.

One reason for explosive growth of mobile devices in the workplace is the realization that mobility makes staff more productive. Another is that workers want to use the same devices they use in their everyday lives for work purposes.

Spurred by work mobility and the bring-your-own-device (BYOD) trend, organizations need to evaluate their situation and begin drafting detailed mobile policies. Well crafted policies protect both the organization and individuals by clearly stating expectations and responsibilities concerning devices and the entity-owned and personal data on them.

Table of Contents

Mobile Revolution

The growth in mobile technology and mobility is omnipresent. Consequently, the need for a solid mobile policy has never been greater. Consider the following:

- The BYOD model is attractive to workers and organizations. Workers benefit from the comfort of using one device for everything. Entities benefit because they often don't have to pay for the devices nor service plans.
- A growing global workforce is spurring mobility. It requires workers to be able to securely access relevant data and applications from a variety of mobile devices at any time.
- Comfortable with mobile devices, users are accessing more applications – a practice that can open the door to security risks. Therefore, organizations are beginning to provide users with approved apps, increasing the need for entity-specific application stores or app distribution solutions.
- Even with the explosive growth of mobile devices in the workplace, relatively few organizations have policies in place to effectively integrate mobile devices into work processes.

While each mobile policy will likely take a custom format, here's a starting point offering components to consider.

The Nuts and Bolts of a Mobile Policy

Although the specifics will differ for each organization, depending on a variety of factors including sector, size and regulatory issues, all mobile policies should contain sections addressing the following:

- Device specification
- Applications
- Mandatory security controls
- Liability and ramifications
- Usage and access of devices
- Access to organizational data
- Financial terms
- Penalties for noncompliance

Goals and Scope

The mobility policy should start with a statement that explains the goals and scope of its content. Goals should be designed to cover what the policy is expected to do. These can include:

- Add to work-life balance
- Support collaborative work
- Supplement organization productivity
- Improve management of mobility costs
- Enhance data security

The scope identifies who is covered by the policy. For example, this can include:

- Employed workers
- Consultants
- Administrators
- Contractors
- Vendors
- Students

Mobile Devices

The policy should address what devices are owned by the organization for staff use (if applicable). Operating system (OS) designation and levels of support will align with the device provided. Devices brought into the workplace by staff, part of a BYOD initiative, must also be considered (if applicable).

Organization-owned Devices – The policy will describe the devices owned by the organization and provided to staff members, etc. This is often done by aligning workers into groups and assigning each group a type of device. For example, supervisors may be eligible for an advanced tablet and smartphone, while other staff members might be assigned a more basic model of each.

Questions to consider:

1. Who is eligible?
2. Who has access based on job title, responsibilities, etc.?
3. What degree of network access will be given?
4. What are the types and kinds of devices supported (smartphone, tablet, aircard)
5. What device-enabled capabilities should be allowed: text messaging, international calling, personal use?
6. Will both domestic and international wireless plans be required?
7. What about mobile data cost?

BYOD Devices – These are devices owned, paid for and furnished by workers, contractors, students, etc. Explain which devices and mobile OSs the organization will support. This is important because, depending on security requirements, decision-makers may have to limit the choices to those that, for example, support personal identification numbers (PINs), code locks, auto lockout, encryption and remote wipe.

This section of the policy also details level of access to mission-critical applications. For example:

- Data that staff can access on their devices
- Security requirements for worker-owned devices
- Level of support workers can expect from the IT department
- Whether only organizational software applications will be supported
- Management solutions used to secure and manage organizational data accessed in a BYOD environment

A policy might state that all devices can download approved software via a specified portal. However, additional software applications, desired by users, must be on an organization-approved list and be purchased by specific reputable sources. All other apps may require approval from the mobile policy board. The policy also may state that the organization won't support user-added software.

Questions to consider:

1. What type of apps can BYOD users use? Are all available?
2. What degree of network access will BYOD devices be given?
3. What BYOD devices and OS platforms will be supported?
4. What applications should be deployed?
5. How will applications be distributed and managed: downloaded from a site, desktop client or pushed out by IT?
6. Where should apps be made available: in-house app store or a public online store such as iTunes or Google Play.
7. How will secure apps be developed?

Security

Obviously, mobile security is critical. This is especially true for worker-owned devices. Therefore, this section of the mobile policy should be very detailed. Some security factors to consider implementing include the following:

- Password requirements
- Data encryption
- Device authentication
- Virtual private network (VPN)
- Full or selective wipe of devices

If you retain the right to remotely wipe lost or stolen devices, explain whether you will be wiping all data (including personal data) or whether you will use a "sandbox" approach that separates work-related data from personal data, eliminating only organizational information.

If you use a mobile device management (MDM) system to help secure and manage mobile devices, make sure to include the requirement to download the specified MDM system. MDM applications can help organizations support mobile policies by offering many of the following:

- Data protection
- Certificate distribution
- Application inventory
- Device configuration
- Lockdown
- Full or selective device wiping
- Support of in-house app store

Mobile Security Lowdown

These 10 practices represent the best places to start:

1. Craft a mobile policy and thoroughly brief workers upon hiring.
2. Decide who pays for devices: workers or the organization?
3. Have the capability to quickly wipe lost or stolen devices.
4. Be able to enforce screen locks, secure logins and rotating passwords.
5. Put into effect device-side encryption.
6. Enable device-side antivirus software.
7. Be sure to manage configurations and patches.
8. Be able to track and secure sensitive data.
9. Institute visibility into devices as well as network traffic.
10. Determine who will provide support for mobile devices — in-house or outsourced?

Questions to consider:

1. Will IT assist with first-time device setup?
2. Will IT provide first- or second-tier support?
3. Will all devices be supported?
4. What is the level of support for personally owned devices?
5. Will only organizational data and apps be supported?
6. How will the device be managed?
7. Will the device be maintained over the air or through synching with a desktop or web application?
8. How will the device be secured, i.e., passwords, device encryption, remote lock, wipe, sandboxing, etc?

Financial responsibility

This is another important area to address. There are three basic financial models an organization can adopt:

- Direct billing — where the organization buys the device and assumes all expenses
- A fixed monthly reimbursement for device support
- Reimbursement based on worker expense reports

More organizations are using their travel and expense reporting systems to manage mobile expenses. If you have done this, make sure that it is incorporated into the mobile policy. Some of the expense-related provisions that CMG, a telecom expense management vendor, recommends include the following:

- How organizations approve mobile device expenditures
- Whether prior management approval must be obtained before a worker can apply for reimbursement
- How to submit invoices and expense reports

Questions to consider:

1. What does the organization pay for?
2. Who pays for service plans and connectivity?
3. Will the organization reimburse the entire monthly cost, pay a stipend, cover the cost of data plan, etc?
4. What is the BYOD device owner responsible for?
5. Where applicable, what type of international calling and international roaming plan will be offered (voice and data)?

Liability and privacy

These are important topics in all mobile device policies, especially in cases where staff members are using their own devices. The organization is well within its rights to monitor a staff member's mobile activities while the device is connected to the entity's network.

However, where exactly does that end? And what about devices owned by the organization? Is workers' data on those devices considered private? It is important to balance privacy and liability concerns and create a system that minimizes the exposure of personal information.

Some of the wording often used in liability privacy statements includes:

- The organization will not assume liability for personal devices
- The organization will not attempt to access a worker's private data, but may do so inadvertently
- Staff members are personally liable for early termination fees associated with a worker-owned personal mobile device and service plan if they choose to discontinue their personal services prior to the conclusion of their contract.

Questions to consider:

1. On staff-owned devices, is the worker's data private?
2. Is it legally acceptable to wipe organizational or personal data if a policy is violated?
3. Will data be collected? If so, how much data, such as GPS data, should be collected?
4. What is the procedure to address lost or stolen devices that are organization-owned or accessing data in a BYOD scenario?
5. Will the organization enforce the use of a "whole device" password?
6. Should jailbroken or rooted devices be prevented from accessing organizational data and apps?
7. What are the ramifications when a user violates the mobile-use policy?
8. Should different violations be treated differently, i.e., eligibility vs. security vs. acceptable use?
9. How often will the mobile-use policy be reviewed and evaluated by the organization?

Getting started

Whether revamping an old mobile policy that no longer fits your needs or developing one from scratch, the first step will always be laying the groundwork. That means involving department heads in the process, evaluating eligibility and devices, negotiating with carriers and making sure that decision-makers are on board with the plan. At that point, you're ready to start developing the actual plan.

There are many decisions that must be made during development of a mobile-use policy. These include:

- Setting financial policies
- Deciding what devices to support
- Deciding what support levels to provide
- Ensuring that security is tight
- Determining how to best connect policy to process

The next step is, in essence, public relations. That means communicating the policy and educating workers on what it will mean for them. This is often best accomplished by first explaining the salient points of the policy to group managers, and then to groups of staff members.

Project Pilot – Once the policy is completed, it's time to put the policy into practice. It's often best to start with a pilot, especially if this is a new venture instead of an updated policy. Consider starting with staff members who are already interested in or stealthily using their own devices.

Starting with a small group representative of various user and use cases within the organization can help determine what's working and what isn't. It also provides time to collect data to measure benefits and costs. Based on that feedback, policy developers can tweak the policy as needed before rolling it out organizationwide.

The CIO or, in some cases, the chief mobility officer, probably spearheaded development of the mobile policy, in concert with a mobile policy board. That same team may or may not be responsible for managing the policy over time.

CDW: A Mobility Partner That Gets IT

We can help get your staff mobile fast. Because CDW maintains partnerships with leading wireless vendors – including network providers and device manufacturers – we offer a one-stop shop of integrated mobility solutions consisting of software (security and management), hardware devices (smartphones, tablets and notebooks) and cellular wireless activation services.

Regardless of the mobile platform you choose, CDW can step in to help with activation and configuration services. What's more, we can ensure that the apps you want running on workers' wireless devices are installed and configured correctly before they turn them on the first time.

Working with your CIO, management team or IT department, we can design, plan, implement and support comprehensive mobile solutions built around you and your organization's needs.

Contact your CDW account manager to discuss the mobile policy checklist. Call 888.423.2392 or visit CDW.ca/mobility

CDW PEOPLE WHO GET IT CANADA