

GOING MOBILE

Developing an Effective Corporate
Mobile Policy



Going Mobile

The wireless revolution has changed. It's no longer simply about making existing applications accessible remotely. Now the focus is on enabling new applications that don't just augment existing business models, but instead, transform them.

By now, most organizations are clear on the advantages and benefits of wireless data solutions in the enterprise: namely, increased productivity, improved efficiency and improved response times resulting in decreased costs and increased revenue opportunities.

But with these advantages come risks, and most have to do with controlling the data contained on wireless devices and the networks and applications to which they connect. How do enterprises maintain control? Ensure compliance? Prevent information loss or leakage? Mobile enterprises that aren't prepared with answers to these questions are exposing themselves to threats with severe and potentially company-wide implications.

It is no longer enough to rely on ad hoc policies regarding wireless computing. One of the best way for organizations to ensure consistency and security is to develop a comprehensive set of policies.

Why Policies Matter

Mobile computing devices, especially those acquired by individuals, represent a significant data risk to most organizations.

These devices can hold sensitive corporate data and are easily misplaced, stolen or otherwise misappropriated. Second, because these devices are sometimes purchased by individuals, specifications and usage controls are difficult to enforce. It is not uncommon for organizations to have means of preventing the removal of computer equipment, and laptops are often checked for serial numbers and asset tags. However, these policies have rarely applied to smartphones and other mobile devices. In any event, the most valuable component of these handheld devices is generally not their asset value, but the stored data.

Backing up data on smartphones and PDAs is also becoming an issue. Handheld devices are frequently lost or damaged, so data loss and the associated loss in productivity can be a concern. Few organizations provide mobile employees with tools, training or guidelines covering data backup for these devices. This can represent additional cost that is not likely to be budgeted.

IT departments across the globe are wrestling with how to ensure employees follow their company's security policies. Indeed, of all internal security concerns, one of the most worrisome is careless or risky behaviour by employees.

Whose Device Is It?

One of the reasons why wireless deployments can be risky is that they are opportunistic: people are going mobile to suit their own needs, and the security of corporate data may be of secondary importance to them.

A company's goal should be to incorporate a mobile strategy that encompasses the needs of the entire organization and the various groups and teams within it. This will not happen overnight, nor will it happen by accident. It will require a strong set of mobility policies. And yet many organizations have no policies whatsoever.

Device ownership is an important first step. If the company owns the device, when can the employee use it, and what can they use it for? At one extreme are employees who may say, "It's my BlackBerry® smartphone and I will do whatever I want with it." At the other extreme is the company that says, "As long as you are under my roof you are going to use this device only in this manner."

There are four ownership models that an enterprise can choose from:

- individual liable, corporate pay
- individual liable, individual pay
- corporate liable, individual pay
- corporate liable, corporate pay

Companies need to determine which of these models is most suited to their needs, and they should also make these policies fair and reasonable. For example, a company may require employees to purchase their own mobile devices, but at the same time heavily restrict the way these devices are used. In a scenario like this, employees may feel resentful and it will be harder to get buy-in on mobile policies.

The Solution

Among the many security features of the BlackBerry® Enterprise Solution are more than 400 IT Policies designed to assist IT departments in maintaining the level of control they desire.

Available policies include commands that allow system administrators to lock or “kill” a handheld device. If a user has misplaced their device, but expects to get it back, the administrator can render it temporarily unusable. If the device has been stolen, it can be permanently disabled to protect confidential data.

It is important that mobile policies cover these scenarios at a minimum, but there are also many other considerations to keep in mind, including: which applications will users be able to download and install, are there restrictions to using Bluetooth® that need to be considered, will data encryption be mandatory on all devices to protect data at rest, and what will be your stance on media cards, cameras, Wi-Fi® and GPS? Your mobile policy should consider all of these scenarios and more, if it is to be effective in protecting your organization while at the same time ensuring that productivity is not impacted.

What is It Worth?

When drawing up mobile policies, begin by thinking about the value of the information you are trying to protect.

Your company's intellectual property—including not only secret recipes or proprietary information, but also the knowledge of your workers—are extremely valuable in today's information economy. But can an enterprise put a price tag on the information contained on an employee's mobile device? This is a sensitive area and the value of data is hard to quantify; it will vary dramatically with each organization.

Who's Got Your Numbers?

Companies should consider phone numbers an asset when they draft mobile policies. Even if employees own their handheld devices, companies can require them to leave their phone numbers behind if they leave the company.

The cost of telephone services can also be affected by mobile policies. If a company has a centralized ownership structure, where all the bills come into one place, it can control these costs much better. When devices are owned personally and expenses are reimbursed, companies often end up paying much more.

Getting Down to Business

Now that you understand some of the benefits and potential pitfalls of mobile policies, it's time to start writing them.

To ensure that policies will be effective, consider the following:

- Policies should never be written in isolation, because the people who are asked to use or enforce them may have differing opinions. A sole policy writer may also neglect things that are important to others. This is not to be taken lightly: enterprises need to get the right people involved, and should include as many people and groups as is practical.
- A number of factors can hinder the adoption of policies, and an enterprise should do its best to anticipate these hurdles. For example, employees will need to be sufficiently trained in the policies and procedures, as well as the reasons behind them, in order to ensure security. You should also consider your corporate culture. Employees in an informal workplace, for instance, may be less likely to buy into restrictive mobile policies.
- Management should enforce and buy into policies or the implementation of them may be adversely affected. Managers should be careful not to use their own handheld devices in ways that contravene policies, and they should demonstrate that adhering to policies is an issue they take seriously.

It's clear that the rise in the mobile workforce is putting more demand on IT departments for greater access to mobile devices and greater access to corporate datastores through those mobile devices. Responsible organizations recognize the inherent risks this carries, as well as the importance of creating comprehensive mobile policies for their organization. They then take their mobile policies and work to implement mobile solutions that enable control over the mobile environment through the use of IT policies.

Discover the BlackBerry Solution Advantage

With more than 400 published IT policies, the BlackBerry Enterprise Solution helps to provide administrators with control over their wireless solution—through intuitive, comprehensive IT policy management tools.

Group IT Policies

Different wireless users within an organization can have different requirements for security and access to information. One size no longer fits all. To meet this challenge, the BlackBerry solution enables administrators to deploy group policies that reflect the needs of the various users and teams within an organization.

Default IT Policy

Each BlackBerry smartphone, upon activation, is designed to be added to a customizable base IT policy to enable a minimum level of security. From this starting point, administrators can create user groups and easily modify policies to meet the security needs of the organization.

Over the Air Enforcement

IT policy settings can be synchronized and assigned to the BlackBerry smartphone over the air. As a result, BlackBerry® Enterprise Server administrators who need to facilitate large deployments can easily change IT policies on a corporate level without requiring users to cradle their BlackBerry smartphones.

With the BlackBerry Enterprise Solution, IT policies are one-way, server-initiated outbound communications. This helps administrators ensure that each BlackBerry smartphone is compliant — the IT policies are designed so that users can't intervene or prevent a policy from being applied once the administrator has initiated it. As well, IT policies carry unique digital signatures to ensure that only the designated BlackBerry Enterprise Server can send updates to a BlackBerry smartphone.

Malware Control

In the PC world, preventing viruses, trojans, worms and spyware (collectively referred to as "malware") consists of two strategies: detection and containment. Detecting malware can require a huge, frequently updated local database or a constant connection to an online database. This approach works for desktop computers, but not for mobile devices.

The BlackBerry Enterprise Solution focuses on containing malicious programs. The BlackBerry Enterprise Server comes with a multitude of Application Control IT policies that allow the administrator to limit the resources and user data available to a given application. For example, restrictions can be imposed on internal or external domains, the phone, Bluetooth, USB and user data such as email and Personal Information Management (PIM). And because limitations can all be specified on a per application basis, administrators can grant elevated permissions to trusted applications.

Discover the BlackBerry Solution Advantage *(cont.)*

Control over the BlackBerry Enterprise Solution

The BlackBerry Enterprise Solution is designed to provide administrators with control over the solution. With over 400 published IT policies, administrators can establish specific enforcement capabilities around:

- Forcing password use, password complexity and timeouts
- Application availability
- Functions that can be performed within each application
- Bluetooth peripherals and how they connect to the BlackBerry smartphone
- The BlackBerry® Smart Card Reader, for two-factor authentication to the BlackBerry smartphone
- Internet browser availability and capabilities
- IT policy change notifications
- Owner information settings
- Attachment viewing and supported formats
- Backup and synchronization requirements and frequency
- SMS, MMS and PIN to PIN message capabilities
- S/MIME and PGP® requirements
- Private key storage level for encrypted messages
- Content protection strength
- Encryption settings and certificate use
- SIM card control over location-related information and call capabilities, and much more.

BlackBerry IT Policies

For a complete listing of all BlackBerry IT policies, review the BlackBerry Enterprise Server Policy Reference Guide (PDF) at: www.blackberry.com/go/security

Easy to deploy, easy to manage

With the BlackBerry Enterprise Solution, organizations can benefit from deployment and management features that help simplify administration.

- **Role- and group-based administration capabilities** - Help reduce security, operational risks, and administrative overhead by delegating permissions by role and creating administrative user groups.
- **Over-the-air wireless IT policy enforcement** – Helps to provide a fast, cost-effective method for supporting users and managing corporate policies remotely so users don't have to go without their devices and IT does not have to have devices in hand to make changes.
- **Track key device statistics** – Helps to easily monitor third party applications loaded, IT policies applied, device models, PIN, software versions and serial numbers.
- **BlackBerry® Web Desktop Manager** – A web-based application that is designed to lower the total cost of ownership for the BlackBerry Enterprise Solution by reducing the number of BlackBerry software components installed on end-user workstations and allowing BlackBerry smartphone users to install software and manage their devices using any browser-enabled computer.
- **BlackBerry® Monitoring Service** – Helps organizations maintain high availability and high performance of their BlackBerry Enterprise Solution infrastructure by providing administrators with enhanced monitoring, alerting, troubleshooting and reporting capabilities and enabling proactive issue identification and resolution.

It's not surprising that the BlackBerry solution is used globally by large enterprise, government and small and medium business. It provides the infrastructure, security and features to empower lines of business with wireless access to a range of critical business information – email, organizer data and voice, as well as business analytics, Customer Relationship Management (CRM) and other business applications. The BlackBerry wireless solution is ideal to keep organizations connected and collaborating.

Promotional Offers

Get started with promotional offers designed to make it easy to evaluate a BlackBerry solution, before you invest. Deliver ease-of-use and increased mobility to your users with a minimum of effort.

Learn more at www.blackberry.com/go/offers

This material, including all material incorporated by reference herein or made available by hyperlink, is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). When you subscribe to Third Party Products and Services you accept that: 1. It is your sole responsibility to: (a) ensure that your airtime service provider will support all features; (b) identify and acquire all required intellectual property licences prior to installation or use and to comply with the terms of such licences; 2. RIM makes no representation, warranty or guarantee and assumes no liability whatsoever in relation to Third Party Products or Services.

Certain features outlined in this document may require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, BlackBerry Device Software and/or additional RIM/BlackBerry software.

The limitations and exclusions herein shall apply irrespective of the nature of the cause of action and in no event shall any director, employee, agent, distributor, supplier or independent contractor of RIM have any liability related to use of the material.

© 2008 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType® and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used as trademarks in the U.S. and countries around the world. Wi-Fi® is a trademark of the Wi-Fi Alliance. Bluetooth is a trademark of Bluetooth SIG. PGP is a trademark of PGP Corporation. All other trademarks are the properties of their respective owners.