CCMI
Intelligent Telecom Data Solutions

Managing Enterprise Wireless Services to Maximum Advantage

Written by:
Kevin DiLallo, Levine, Blaszak, Block and Boothby LLP and
Ben Fox, TechCaliber Consulting, LLC

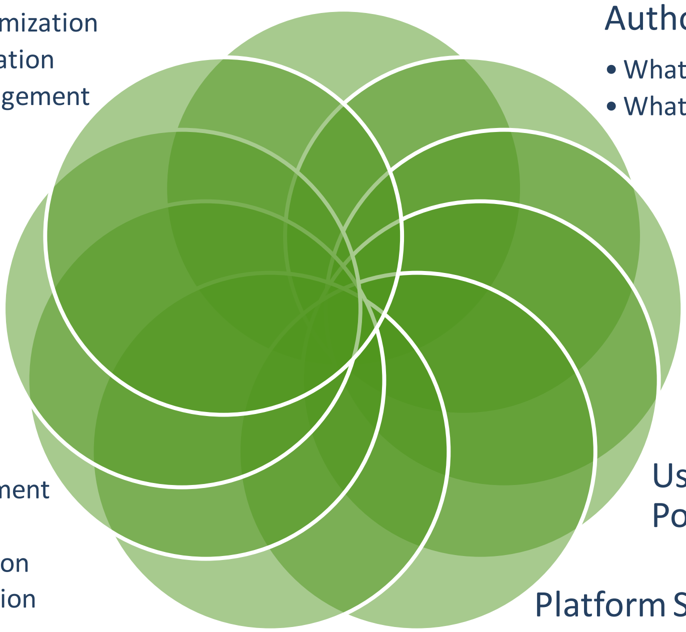
August 2015

Managing Enterprise Wireless Services to Maximum Advantage

You can develop a wireless strategy for your enterprise that will deliver the capabilities your users need while keeping costs under control and managing risks appropriately, but to do it right you have to address a range of interrelated issues.

Deployment of a successful enterprise wireless strategy also requires a comprehensive user wireless policy which is aligned with the enterprise's global mobility strategy and with best practices for the management of the wireless services and costs.

Here's what the process looks like:



Entitlement Policy

- Who should have a device
- What type of device

Authorized Usage Policy

- What usage is not appropriate
- What usage should be barred

Policy Enforcement

- User Communications
- Corporate Mandate
- Consequences
- Controls
- Monitoring

User Reimbursement Policy

Platform Strategy

- Android
- iOS
- Windows Phone
- Application Integration
- Unified Communications

BYOD – bring your own device

Risk Mitigation

- Security management
- Liability for costs
- Legal risk mitigation
- Contract negotiation

Mobile Device Management

Cost Management

- Rate Plan Optimization
- Pricing Negotiation
- Expense Management

I. Entitlement Policy

The Entitlement Policy defines which users should be provided with a corporate funded device, and what types of devices they should be given. Best practice policies address:

- The job/role attributes which require remote/mobile connectivity (e.g., seniority, remote working, business travel).
- Other criteria that need to be met for a user to obtain a corporate funded device (e.g., a particular level of approval for a particular device type – for instance a tablet may require more senior sign-off than a cell phone).
- Minimizing the number of devices each user carries (e.g., encouraging the use of tethering services and mobile hotspot capabilities of smartphones as an alternative to getting users a smartphone *and* a data card).

II. Authorized Usage Policy

The Authorized Usage Policy addresses the types of usage permitted under the policy, plus the manner in which wireless services should and should not be used for company business. Best practices include:

- The Authorized Usage Policy should be provided to users when they receive a corporate device or are granted permission to begin submitting expenses for mobile costs incurred on personally owned devices and plans
- Requiring users to formally confirm that they have read and agreed to abide by the Authorized Usage Policy.
- Identifying the types of usage that are prohibited or not reimbursable. Areas to address include premium rate calls/texts, unreasonable levels of non-business usage, pay-per-call directory assistance services, mobile payment services, charitable contributions via text, application purchases and services (including navigation services), ring tones and information services charged to the wireless bill.
- Responsible use of mobile services. For example it is best practice to specifically prohibit the use of wireless services while driving (see Risk Mitigation).
- Security considerations – e.g., mandatory use of PINs; strong password policies.

III. Policy Enforcement

A common failing of wireless policies is lack of enforcement, or the lack of corporate mandate to deploy and implement the approved wireless policy.

These failings often lead to users' only paying lip service to the policies, or to not even be aware that a policy exists. Addressing the approach to communication and enforcement of the wireless policy is crucial:

- The wireless policy should have a C-level executive sponsor. A senior sponsor gives the wireless policy authority and minimizes objections and exceptions requests (particularly with regard to the Entitlement Policy).
- Proactive communication of wireless policies to users is very important. This applies not just to the Authorized Usage Policy, but all policies that have direct user impact (including policies governing Entitlement, User Reimbursement, Enforcement and – if permitted – BYOD.
- Communicating best practices, and the logic behind them, as well as the "do's and don'ts" is also important. For instance, users often do not realize how much international roaming costs – if the high cost of such usage is explained good corporate citizens will proactively use alternative options – such as a land line in the international office to which they are travelling – rather than just defaulting to their wireless device.
- The Authorized Usage Policy should be underwritten with HR-endorsed remedies (e.g., formal warnings) for abuse. It is important that there be consequences for abuse.
- An important best practice is to monitor compliance, even if only on a spot-check basis – compliance with any policy increases dramatically when users are conscious that their adherence to the policy is being monitored.
- Where possible, wireless policies should be automatically enforced – for example suppliers can bar users from certain types of usage (e.g., purchasing applications on the corporate invoice; blocking international usage for users who are not eligible for calling internationally). Such features and capabilities should be leveraged. Mobile Device Management tools can also enable the automatic enforcement of certain aspects of the Authorized Usage Policy.

IV. User Reimbursement Policy

The primary policy decision in terms of User Reimbursement is whether to permit or prohibit users from expensing their personal wireless costs. Best practice is to prohibit users from expensing personal wireless expenditures. The main exception is for users who are permitted to expense specific portions of their personal wireless expenses – e.g., international roaming costs when travelling on company business. Otherwise, users should not be permitted to expense personal wireless costs, and if the company expects employees to use wireless services on the job, the company should be the party contracting with the service providers.

A range of benefits are unattainable except where the company is contracting for the wireless service. In particular:

- Large enterprises can negotiate preferential pricing compared to individual customers.
- The enterprise can retain far greater control over the wireless services when it is providing users with corporate devices, rather than reimbursing the cost of personal services (e.g., moving users between different rate plans; obtaining detailed management reporting from the wireless service provider; barring usage prohibited by the Authorized Usage Policy).

V. Platform Strategy

Many enterprises now support a multi-platform environment that cuts across a range of smartphones and tablet form factors.

It is important that the platforms and devices that an enterprise's IT department supports are documented in the wireless policy, not least to set users' expectations. The Entitlement Policy should address who qualifies for different device types/platforms.

The key best practice in this area is to pro-actively develop a strategy for the platforms and devices that will be supported, based on consideration of various factors:

- Scope of end-user support to be provided;
- How end-user support will be delivered;
- The management tools required to effectively manage different platforms and devices;
- The cost impact of different platform/device choices;
- Impact on user behavior and consumption (e.g., 4G devices tend to generate substantially more data usage than 3G devices);
- Integration with corporate applications;
- Alignment with the enterprise's Unified Communications and Collaboration strategy.

VI. Bring Your Own Device (BYOD)

The original philosophy for BYOD was to enable users to use their personal devices to connect to corporate applications. Productivity benefits and satisfied users were touted as the key benefits, and the costs of enabling that access (with appropriate security – see Mobile Device Management below) were said to be modest.

Over time, BYOD has also been touted as a potential cost savings opportunity, essentially by removing corporate provided and funded devices from users and forcing them to use personal devices instead. Whether or not BYOD drives cost savings is hotly debated, but we can say with some confidence that there is little chance for savings if BYOD leads to abandonment of the User Reimbursement Policy best practice of prohibiting users from expensing personal wireless costs.

Similarly to the Platform Strategy, the key BYOD best practice is to pro-actively develop a strategy, and to document the resulting policy so that it can be formally communicated to users. In developing the BYOD strategy, key considerations include:

- Which mobility platforms will be approved for BYOD?
- Which corporate applications will be accessible to BYOD users?
- What (if any) end-user support will be provided to BYOD users?
- What management tools are required to enable BYOD?
- What costs are associated with enabling BYOD?
- Which security risks does BYOD pose to the enterprise and its customers?
- What rights will the enterprise require with respect to corporate data on BYOD devices (e.g., remote wipe capabilities)?

Most BYOD implementations entail deployment of a Mobile Device Management (MDM) solution that gives the enterprise some control and management capabilities in relation to user devices. A key wireless policy best practice in relation to BYOD is to require BYOD users to agree that they will allow their personal device to be managed by the MDM solution, and grant the enterprise rights to perform operations such as remote wipe of corporate data when necessary (e.g., if a device is lost, or the user leaves the company).

VII. Risk Mitigation

Risk Mitigation should be a dominant theme throughout an enterprise's mobility strategy and wireless policy development. Key concepts and best practices include:

- Adopting Authorized Usage Policies designed to minimize the enterprise's liability for employee negligence and irresponsible or illegal use (such as driving while using a wireless device; copyright infringement; or harassment).

- Security considerations. For example, the policy should mandate the use of PINs/passwords on devices and identify the categories of sensitive corporate data that can, and cannot, be stored on or transmitted from wireless devices.
- Supplier contracts that appropriately balance legal risks and support obligations between the supplier and customer and are aligned with the enterprise's wireless policy.

XIII. Mobile Device Management (MDM)

MDM solutions used to manage "smart(er)" devices are offered by many vendors, including Sybase, Good Technology and MobileIron. The demise of BlackBerry has been a key catalyst for the growth in MDM, which typically supports multiple device platforms (iOS, Android, BlackBerry and Windows Mobile) via a single application/solution.

MDM provides important security capabilities such as remote wipe, pushing out patches and applications, and security policy enforcement (e.g., strong password requirements). MDM can also be used to monitor and enforce the Authorized Usage Policy, such as barring and monitoring different forms of usage, performing usage reporting, and managing users' ability to use different capabilities (e.g., placing international calls).

MDM solutions are now a standard feature of enterprise wireless strategies, and an important precursor of BYOD implementation.

Key capabilities to look for before selecting an MDM solution include:

- Multi-platform, device diversity;
- Cloud-based service;
- Breadth of functional capabilities:
  - Policy Enforcement;
  - Security and compliance implementation;
  - Containerization;
  - Inventory Management;
  - Over-the-air software distribution, patching, updating;
  - Administration and reporting.

IV. Cost Management

Many of the wireless policy best practices described above address cost management. But in order to drive market leading mobility costs, a wireless strategy must include best practice cost management as a separate area of focus:

- Strategic sourcing – wireless contracts should be kept short (best practice is two years or less) and competitively sourced regularly to remain current in a very dynamic market.
- Rate plan optimization – regular reviews are crucial to confirm that each of your users is using the most cost-effective plans and features available under the contract for his/her individual usage profile and needs. Performing rate plan optimizations on a quarterly basis is best practice. It generates substantial savings without any change in vendors or equipment.
- Expense management – rate plan optimization reviews should be combined or supplemented with expense management and billing reviews to verify that users are being invoiced correctly in accordance with the applicable contract. More and more enterprises are using wireless Telecom Expense Management (TEM) companies to assist with this, but TEM complements in-depth billing reviews; it doesn't replace them.