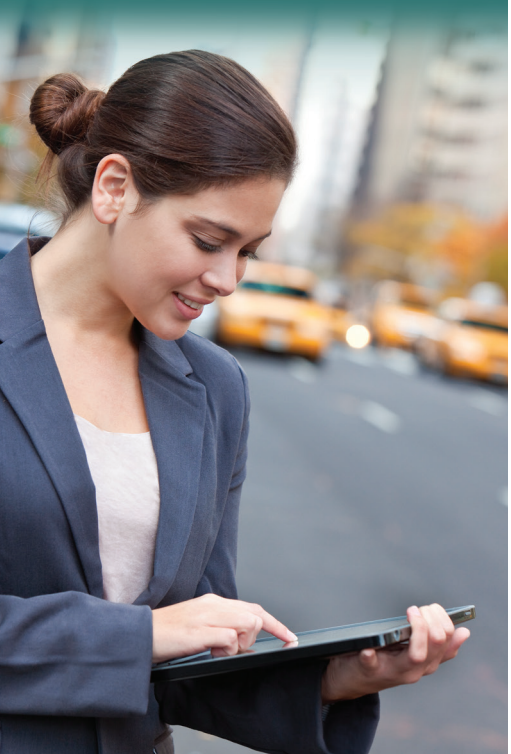
Apple Mobility for Enterprise

The number of organizations deploying Apple® mobile devices is increasing exponentially. PCMG will show you how to manage these deployments, enhancing productivity and decreasing IT involvement.

Call your Account Executive today to learn more.

800-625-5468
pcmg.com

Authorized Service Provider



PCMG can empower your team with anywhere-access to the tools they need to stay successful on the road.

Comprehensive support for iPad, iPhone, and iPod touch

The proliferation of tablets and smartphone devices has forced IT managers to contend with new mobile security risks. 70% of respondents to the InformationWeek Analytics 2011 Strategic Survey stated these mobile devices pose some level of threat to their organizations' security today with another 20% expecting trouble down the road.[1] The two most cited concerns are that sensitive information will remain in the possession of someone who leaves the agency, or it will be on a device that is lost or stolen.

Although initial IT costs go down with policies such as Bring-Your-Own-Device, these gains come with additional pressures on IT departments. Fortunately, IT has recourse: Mobile Device Management can manage and mitigate these challenges via secure provisioning and device accountability.

Local Control for Distant Devices

Managing mobile technology at the enterprise level helps ensure both the security of the network and the protection of agency data. Deployed mobile devices can be activated on-the-fly via SMS, e-mail, or using a Web-based interface. These options allow devices to be enrolled into a solution using authenticated user credentials, which instantly configures settings and access to enterprise accounts.

Once enrolled, these devices can be provisioned for various levels of security, including mandatory pass codes, remote lock-down, audit trail generation, and quickly identifying non-compliant devices via monitoring. With configured alerts, IT can be notified of issues immediately and through periodically generated reports.

With the ability to manage devices individually or in groups, IT can make granular or broad updates, changes, and settings adjustments over the air — all without any user interaction.

Satisfied IT Departments

The consumerization of technology has complicated the duties of IT, who must meet the new and varied demands of the users while setting security standards. Enrollment in a Mobile Device Management Solution allows users easy access to applications that they need to perform their duties and streamlines the enforcement of your organization's mobile device policy. By increasing the number of mobile device choices, we gain user acceptance on which tools to use.

Satisfied End-Users

Beyond security and stability, one of the key factors to Mobile Device Management is the superior user experience. With many of the elements of the infrastructure and access tied into the profiles, users no longer need to manage this information. With profile-configured VPN and network access, users do not have to hunt for agency access and Wi-Fi keys. E-mail, contacts, and calendars configured by profile ensure that every user has access to their resources immediately. With Web Clips, we can immediately provide access to agency sites, from HR to Operations and even Application catalogs.

[1] *Source: InformationWeek (http://www.informationweek.com/news/mobility/business/229402912)*

PCM-G
PC MALL GOV

DS100620REVA122012

iPad deployment workshop: A week of planning, a future of success

Achieving Success

Thanks to PCMG's long-standing relationships with Apple and other vendors, we can provide a full start-to-finish solution to help you be prepared for deploying Apple mobile devices in your organization. Our intensive five-day, hands-on seminar starts with a detailed analysis of your existing infrastructure and then guides you through the entire process of reviewing the environmental factors that influence a successful deployment, understanding the possibilities of Mobile Device Management, and determining the key requirements for a successful Proof of Concept in your particular organization's environment.

Day 1
Analysis

- Directory Services
- Networking
- Security
- Messaging
- Web and File
- Virtualization

Day 2
Deployment

- Capabilities
- Limitations
- Processes

Day 3
Scenarios

- Business Integration
- Security
- Configuration and Deployment
- Application Development and Distribution

Day 4
Review

- Requirements of Mobile Device Management
- Environmental Analysis Review
- Environmental Recommendations
- Analysis of MDM Solutions

Day 5
Policies

- Existent Policy Review
- Policy Paradigms and Considerations
- Policy Workshop

PCM-G
PC MALL GOV