white paper

WHITE PAPER

Policy Driven Approach to Mobile Device Management in Government

Managing the Complete Lifecycle of Global Communications

Tangoe, Inc.
35 Executive Blvd., Orange, CT 06477
Tel: 203-859-9300 • www.tangoe.com

G2SF, Inc.
11921 Freedom Drive, Suite 550
Reston, VA 20190
Tel: 571-281-1737 • www.g2sf.com

EXECUTIVE SUMMARY

The following describes the process by which policy outcomes are developed through the Mobile Device Management (MDM) implementation solution, along with the technology behind a workable solution for applying Mobile Technologies within commercial enterprises and Government Agencies. The purpose of this white paper is to enable other groups and organizations to leverage knowledge of this process and also to demonstrate a capability for policy management within a dynamic IT environment. Further questions include how will organizations respond to faster IT development, and do security and process bottlenecks occur as the demand for IT services increases? This white paper also provides a detailed list of the six key critical areas in the management and security of mobile devices and their data. A MDM solution is mission-critical for millions of IT professionals around the world both commercially and in the Government.

ANALYSIS

Mobility Policy Management

Effective Mobility Policy Management (MPM) begins at the top of an organization with leadership determining policy development and management as an organizational priority. The following key critical areas are the next steps to help set the course for MPM.

1. Identify Stakeholders

An organization's mobility policy tends to evolve as various stakeholders, who previously were not interested in workstation policy, become interested in mobility policy. Most organizations have a Chief Information Officer, Chief Security Officer, and other common stakeholders. When identifying other stakeholder candidates, consider pinpointing service champions who have both a particular interest in the policy development of mobility and have notable influence over the organization. Other parties, such as members from counsel/legal, organizational unions, asset management, and field user representatives, should also be considered.

When evaluating preferred stakeholder qualities, a good distinction is a candidate's level of awareness about tablets and mobile access, in turn, they will probably care about the policy that governs them. Consequently, making this distinction a standard for stakeholder identification synthesizes key stakeholders and all interested parties.

2. Identify Business Requirements

Organizations' mobility requirements tend to be very fluid. We recommend that organizations manage business requirements with frequent "check-ins" to confirm that requirements are still valid.

3. Prioritize Requirements

Prioritization of requirements are equally as important as identifying. Requirements should be

revised frequently to ensure that the fluidity of the mobility environment is effectively managed.

4. Negotiate Requirements

The process of negotiation can be lengthy, so discussions, information sessions and workshops are all important tools to enable stakeholders to feel included and provide their feedback. How inclusive the negotiation process is will vary by the organizational culture. Simultaneously, the more inclusion in the process, the more likely the mobility policy will succeed in terms of adoption, and eventually, overall security and data management. We suggest making the investment to include all stakeholders be made upfront to maximize as much consensus as possible, thereby resulting in successful adoption and adherence rates.

5. Finalize Business Needs and Relate Requirements

The process of substantiating business needs to the project requirements is imperative to validate that policy and confirm that business needs connect. A requirements matrix is a valuable tool in the policy development effort. It can be used as a reference when questions arise as to why policy decisions were made, and to provide clear context for mobility policy discussions.

6. Develop Mobility Policy and Updates to Existing Policy Per Established Processes

Once all stakeholders agree on what should be in the policy plan, newly created, updated and/or revised policy statements will be cross-referenced with existing established processes to identify any interdependencies or constraints. We also recommend that this process include various stakeholders to improve successful adoption and adherence rates.

Common Challenges to Mobility Policy Management

Mobility is more fluid than most other IT environments, as a result, working with mobility policy and mobility IT project implementation encompasses a unique set of challenges discussed below.

1. Various Stakeholders with Varying Business Needs

Mobility tends to elicit the interest of more stakeholders than other IT environments, mostly due to cultural and novelty trends. Whether the goal is to increase geographic flexibility, added capabilities, provide similarity to commercial interfaces, gain convenience, or other interests, most organizational members will be interested in contributing their feedback and perspective to the mobility policy outcome. Managing these interests will vary by organization. We recommend an inclusive process to develop the “best-fit” policy for the organization.

2. Organization Silos May Not Facilitate Convergence Towards a Solution

Some organizations still have entrenched silos that are political, personality, or leadership driven. These silos, though they may have maintained a standard accountability process within the organization, tend to disrupt, delay, and reduce the effectiveness of policy deliberations. We recommend that clear expectations be defined to stakeholders and other contributors in order to limit silo dynamics. The degree of limitation will vary by organization, and directly affect the expediency and effectiveness of policy deliberation. Additionally, silo dynamics have a high impact on how pleasant or unpleasant the process is for the people actively participating.

3. Mobility Context Changes More Rapidly Than Other IT environments

The fluidity of the mobility environment compels leadership to constantly re-evaluate business decisions, risk analysis, core objectives, and tactical approaches against other IT environments. We recommend keeping an open mind towards a flexible approach that is open to iterative and managed-modifications.

4. Various Organizational Perspectives on What “Policy” is and Who Authoritatively Defines Mobility “Policy”

Frequently the term “policy” means different things to different people, and has a different impact on organizational groups. We recommend managing expectations early in the policy development effort by clarifying the definition of policy, determining the standard process for developing and implementing policy, and defining how closely the mobility efforts will follow the standard process.

<u>Mitigating Actions for the Challenges to Mobility Policy Management</u>

Our mitigation strategies for the stated challenges to mobility policy include:

1. Effectively Define Roles and Responsibilities

The fluidity of the mobility environment compels stakeholders to effectively manage roles and responsibilities, while maintaining flexibility in these assignments as the mobility effort progresses. Frequently variations in project needs will create a need for re-evaluation of roles and responsibilities. We recommend defining roles and responsibilities early on, and revisiting them with all stakeholders on a periodic basis.

2. Establish Clear Expectations for Contributions

It is important to clarify expectations regarding participation and contributions during the policy working groups, discussions, workshops, and other functions. Defining writing assignments, research and collaborative writing goals should all occur early on for best results. Maintaining a schedule for contributions may also help everyone meet defined milestones. We recommend managing expectations for policy contributions to maximize group effectiveness.

3. Effective Discussion and Meeting Facilitation

During the policy negotiation phase, it is important that meetings, discussions and workshops

remain inclusive. Participants must be engaged and feel that their contributions are valued. We recommend implementing all rules regarding running effective meetings during this phase to ensure the maximal inclusion potential and meeting productivity.

4. Adherence to the MPM Plan and Agreed Upon Timeframes

The effective management of the MPM plan's schedule and milestones provide value to the overall effort of developing a MPM plan. We recommend a robust project management plan to develop and implement mobility policy.

Process Development

This section highlights the areas of process development that require particular attention for effectively integrating mobility services into the enterprise.

1. Design Mobility Procedures to Plug-in to Existing Processes

Mobility procedures should integrate into existing processes and procedures where possible. Therefore, we recommend a maturity analysis of existing processes to help identify the interface between new mobility processes and existing IT service processes.

2. Develop Ad Hoc Processes in the Interim When Needed

Interim processes should be developed to connect existing processes to mobility processes where tactically feasible. The iterative nature of process development means that these ad hoc processes may be revisited when focusing on a specific process. We recommend that the mobility process development effort define a plan for building ad hoc processes early on along with an overall process development and integration plan.

3. Key Interfaces Between Existing IT Service Processes and Emerging Mobility Processes

Some IT processes will interface more with mobility processes than others. We suggest particular attention to the following Information Technology Infrastructure Library processes: Request Fulfillment, Incident Management, Event Management, Service Asset & Configuration Management, among others.

4. Involve Process Owners in the Development of New Procedures and Updates

Process owners should be heavily involved in the development and administration of new process efforts. Prior to any process development efforts, process owners should be identified and assigned to a process area. We recommend enabling process owners to contribute heavily to the development of new mobility processes.

5. Train All Personnel on Business Priorities of the Service and Procedure Changes and Updates

Developing effective training materials will significantly improve the effectiveness of new process adoption and adherence. We recommend that organizations invest in resources that

will help develop detailed training plans that will be made available to all staff that interface with the new processes in addition to resources documenting business priorities.

6. Monitor Process and Procedure Development and Maintain the Process Development Plan

Monitoring of process development is key to ensuring that the fluidity of the mobility environment is effectively managed by new mobility processes. Frequent check-ins and re-evaluations are helpful to continuously improve mobility processes, whether ad hoc or permanent. We recommend inclusion of stakeholders in process development and implementation and frequent opportunities for participants to offer feedback and suggestions for improvement.

The MDM Offers a Seamless Policy Management Experience

The MDM solution consists of a mobility ecosystem that includes Applications, Containerization, and Content Management at its core to secure and manage all mobile devices and operating systems within the corporate or government environment. The MDM process supports the entire mobile lifecycle and its core functions include:

- End-User Self-Activation

Provides a Self-Service Portal that increases end user adoption and satisfaction by reducing IT and help-desk work cycles.

- Security and Policy Compliance

Maintains security and policy compliance from a single global web-based console. Monitoring capabilities include device usage statistics, enforcing security policies, securing mobile access to corporate resources, tracking lost devices, and remotely locking and wiping iOS, Android, BlackBerry, and Windows devices.

- Containerization

Creates a secure corporate workspace container to enforce security policies for enterprise data, communications, and applications on a mobile device (smartphone or tablet) while also separating corporate data from personal data and applications.

- Application Management

Deploys, upgrades, updates and removes IT approved public and custom-built applications for iOS, Android, Windows, and BlackBerry mobile devices.

- Content Management

Secures Containerized access to enterprise content with policy controls including view, edit, delete, print, share, and more.

- Real-Time Expense Management

Reduces the risk of bill shock by tracking device data, voice, and SMS usage in real-time against preconfigured individual and pooled carrier plans' usage thresholds. Real-Time Expense Management capabilities can:

- Block unapproved devices from accessing enterprise resources such as Exchange and the application portal
- Manage and enforce mobile application policies across device types and liability models to reduce risks from potential security breaches and data leakage
- Configure secure email policies that prevent unauthorized forwarding, cut and paste and sending unencrypted data
- Consistently enforce your IT team's usage and management policies automatically across the device fleet with the MDM patented rules engine.
- Monitor device usage against carrier rate plans in real-time which can save budget dollars by preventing bill shock
- Reduce security and cost risks when a device is lost or stolen by tracking its location and enforcing your security policies

Security and Policy Compliances

The MDM solution provides the capability to configure device settings automatically and intelligently with our patented Rules Based Framework. Our Framework allows administrators to define policies on specific platforms and/or device types, and to enforce policies, applications, as well as monitor devices based on user (AD/LDAP groups, OU's departments, business units, etc.), and device (device liability, jailbroken/rooted status, make, model, OS version, memory, battery, roaming status, voice/text/data thresholds etc.) criteria.

The MDM solution is designed to create enforcement rules based on company business rules, for example:

- Every user with a corporate iPhone in Sales will have apps 'XYZ', encryption, strict password policy, and Salesforce app; but personally owned iPhones in Sales will be enforced with a rule for a strict password and Salesforce app
- Sales employees with Androids will have a different configuration
- Accounting employees will have different configurations

The MDM solution gives IT leaders the ability to deploy and control large numbers of mobile devices anywhere in the world using a single global web-based console. IT leaders can easily enforce security policies and compliance, secure mobile access to corporate resources, track lost devices, and remotely lock and wipe Apple, Android, BlackBerry, and Windows mobile devices using this web-based console. End-users get fast activation on their device of choice while enterprises easily manage thousands of mobile devices and applications.

Integration between the MDM and Tangoe's Wireless TEM portal provides a seamless user

experience for end-to-end mobile policy compliance.

- The MDM console receives carrier plan details and updates in real-time from Tangoe's Wireless TEM portal as well as plan-based alerts.
- The Wireless TEM portal receives application lists, device memory status, and real-time usage statistics from MDM.
- Only approved devices for procurement are provisioned with the appropriate usage, management and security policies when accessing enterprise resources.

Content Management

The MDM Content Management solution addresses Data Loss Prevention (DLP) on mobile devices. MDM supports data synchronization which can enable a secure file container (or zone) on the device so that users can have access to all of the files, documents, PDFs, media from file shares, mapped drives and/or SharePoint. This container can be controlled so that no information can be cut, copied, or pasted outside of the container; and no information can be forwarded or opened by another program outside of the container. All content would remain within the enterprise environment and not temporarily stored in Tangoe's environment. Administrators can control which applications have access to read and/or edit information from the container. The container can be selectively wiped if the device is lost, stolen, or decommissioned.

Secure Collaboration for Your Mobile Workforce

Securely collaborating in a mobile environment gives workforces the ability to:

- Connect to all enterprise document repositories as they would when in the office
- Obtain instant access to the most current documents from personal devices
- Experience a robust VPN
- Share easily
- Use trusted apps on personal devices
- Comply with end-to-end governance with no compromises to corporate data and regulatory requirements
- Bring their own devices (BYOD) with personalized apps
- Leave their computers at home to avoid using high-risk consumer cloud storage
- Keep organizational data safe
- Lower support costs

Containerization

As a mobile-centric company, Tangoe understands that a successful BYOD solution for mobility presents unique challenges like, device fragmentation, the privacy and governance over the content stored on a mobile device, and security and management concerns. These challenges are addressed, through the Tangoe Containerization process, to maximize the benefit to all

stakeholders in the ecosystem which include employees, employers, wireless carriers, and device manufacturers. Containerization empowers users with unrestricted device choice that fits the full range of their personal needs while enabling them to have secure access to their enterprise data, and also protecting their privacy.

By providing dual persona profiles, the Containerization platform secures business applications from potentially breaching personal applications by architecturally eliminating the need to wrap each business application in a shell to protect it. Standard applications execute in native binary form providing unrestricted application choice.

The Containerization process delivers the following important benefits to employees and organizations:

- Maximum business application choices
- A carrier- and device-agnostic client that is downloadable for each product family
- Maximum device choices
- High application agility in dual persona profiles
- Executes on non-rooted, stock operating systems and scales across an entire device family
- Government grade secure container that isolates business applications from threats
- Management and client safeguards to protect employee privacy
- Comprehensive infrastructure-less management and security consoles for both user and IT
- Assurance that enrollment in the organization's BYOD program will not jeopardize any employee personal and private data such as pictures, birthdays, and contacts, and when necessary, corporate data can be removed safely without harming any personal information.
- Encrypted corporate data using the most sophisticated, FIPS-140-2 certified encryption algorithms, protect against malware and prevent unauthorized access via security policies that are tailored by employee group and securely distributed OTA (over the air).
- Enables secure, employee-friendly, BYOD programs combined with data leakage prevention policies by permitting 'personal data' to co-exist on the same device with corporate applications while maintaining logical separation of corporate applications and data from personal applications and data.
- Prevent personal applications from accessing enterprise data
- Deploy container policies including copy and paste restrictions for data, application install and removal controls, and anti-tamper (root and debugger) support
- Scale across an organization's fleet of Android and iOS devices to provide a consistent user experience through one central portal

Application Management

The Application Management process can provide your organization with the ability to reliably

make applications available to your organization's smartphone devices in an intelligent and automated manner. Organizational decision-makers will be able to eliminate the administrative labor associated with application deployment to your organization's mobile community, and also significantly diminish the amount of reactive support that is usually required for such activities.

Mobile Enterprise Application Distribution and Management

The MDM mobile enterprise and application distribution and management process includes:

- OTA automated deployment and installation of required applications via APNS (Apple Push Notification Service)
- Deployment rules that can include device OS, download via Wi-Fi (and not via cellular) connectivity, and minimums for battery life and available memory
- Deployment of required and recommended internal applications OTA across your enterprise and managed by secure user access to the Enterprise App Portal
- Blacklist and whitelist applications and enforce compliance with the Automated Rules Engine and the MDM on-device client reporting application inventory
- Rules-based monitoring for the presence or absence of an application:
    - The MDM rules engine can now automatically change device features and functions based on the presence or absence of an application. For instance, if a device has a blacklisted application, the device can be prevented from accessing Exchange and the Enterprise App Portal.

Enterprise Application Portal

Tangoe enterprise application portal capabilities include:

- Employee-driven requests and the ability to deploy enterprise and approved 3rd party applications on-demand from their smartphone, tablet or the MDM Self-Service Portal that is integrated directly with public "app" stores for IT approved applications
- On-demand access from the iOS and Android clients and the Self-Service Portal
- Administrator-driven ability to disable the Enterprise App Portal for individual liable users
    - This feature strengthens security policy compliance rules by preventing access to enterprise applications and storing app data on an individually owned (IL) device.
- Applications that can be deployed on-demand OTA via SSL
- The ability to authenticate users before allowing them to view and download enterprise apps
- The ability to ABQ – Allow – Block – Quarantine access to the Enterprise Application Portal and Microsoft Exchange if an application is not installed or if a blacklisted application is present
- Generation of application inventory, version history, and compliance reports for application lifecycle planning, policy enforcement and management
- The ability to detect employees whose devices are Jailbroken or Rooted and

automatically prevent those devices from accessing the Enterprise Application Portal

- Support Apple's Volume Purchase Program includes importing redemption keys (purchased from Apple) into an MDM app profile, automatically manage the upload, storing and distribution of redemption codes, remove private and 3rd party apps, and force password use to purchase applications from iTunes App Store.
- Exception reports for devices whose applications were not properly installed
- Ensures apps are deployed to the correct device OS, and that the device has enough battery and memory available.
- Exception reporting for devices that do not meet minimum requirements for the application to be deployed.

CONCLUSION

As mobility gains popularity within the corporate enterprise and Government Agencies the management of those devices becomes critical and the security of the enterprise is at risk. It is therefore crucial that IT departments take a measured 'Policy Driven' approach to implementation of a MDM solution in addition to taking advantage of proven technology solutions currently on the market. G2SF Mobile Solutions Practice has years of practical experience implementing and managing mobile solutions within Government and has used "Best in Class" technologies with our policy driven approach.

The MDM is unique in that it is the only MDM solution that offers its own in-house fully Managed Services and End-User Support model on top of the software. This ensures that both your mobile user community and the infrastructure they rely on are well-supported, secure, and stable.

The MDM service solution allows enterprises to easily and quickly leverage all of the powerful features of Tangoe's MDM software. Tangoe's MDM Services Team has over 10 years of experience in helping customers manage their mobile devices and delivers the solution both as a cloud-based model and remotely for customer-premise MDM instances.

The MDM solution has been designed to support both Corporate Liable devices as well as IL devices.

The MDM solution can be delivered as an on-premise solution or as a hosted SaaS type model. Recently the shift has been from enterprises deploying our solution behind their firewall to a hosted solution, however Tangoe is very flexible as we understand organizations often have different requirements.

Through Tangoe's robust MDM feature set, enterprises can reduce IT support and labor costs for mobile devices by more than 50 percent. Enterprises can proactively prevent costs BEFORE they are incurred with comprehensive capabilities at the server and device levels, and monitor and minimize costs in real-time. Tangoe's MDM solution enables enterprises to control costs throughout the entire lifecycle of their mobile devices.

Global organizations depend upon Tangoe's technology-enabled managed services and patented technologies to optimize and manage the lifecycle of their fixed and mobile enterprise communications resources.

ABOUT TANGOE

Tangoe is a leading global provider of Communications Lifecycle Management (CLM) software and related services to a wide range of global enterprises. CLM encompasses the entire life-cycle of an enterprise's communications assets and services, including mobile device management, telecom expense management planning and sourcing, procurement and provisioning, inventory and usage management, invoice processing, expense allocation and accounting, and device recycling. Tangoe's Communications Management Platform is an on-demand suite of software designed to manage and optimize the complex processes and expenses associated with this lifecycle for both fixed and mobile communications assets and services. Tango's customers can also manage their communications assets and services by engaging Tango's client service group.

Additional information about Tangoe can be found at www.tangoe.com. Tangoe is a registered trademark of Tangoe, Inc.

ABOUT GS2F

G2SF is an IT Service Management, Engineering and Sciences, Consulting Firm providing quality support to the Federal Government, State and Local, Defense and Commercial Markets since 2008. Headquartered in Reston, VA the company has built its reputation on an unwavering commitment to a diverse customer base, valuable partnerships within the public and private sectors, and a dedication to recruiting and retaining only top performers. G2SF is currently certified as a participant in the program for the US Small Business Administration (SBA). G2SF has gained recognition as a one-source IT solution company, offering a wide array of IT Service Management, Mobil Solutions, Program Management, Professional Services, Training, and Engineering Services. Our IT Service Management Consulting Practice supports the day-to-day operations of many of our customers' IT operations from the functional to the highly technical such as IT Infrastructure and Program Support Services.