



# Mobility In Government Services

## A Checklist Towards Regulatory Compliance

## Mobility in Government Services: A Checklist for Regulatory Compliance

Government organizations and their agencies, partners and suppliers are under intense pressure to wring maximum value from taxpayers' money – which means tapping in to new tools that can help increase productivity, drive efficiency, improve service and cut costs. Innovation in the mobile space has created a host of new opportunities for government departments to accomplish all of these goals, and more.

But with innovation comes risk. And risks are unnerving to groups that are mandated to safeguard the assets of the people they serve, and to maintain the highest standards when it comes to protecting data and communications. In the mobile space, as smartphone capabilities grow, so do employee expectations about leveraging those devices to get work done when and where they choose. But more mobility means that confidential data and sensitive communications, once only accessible through hard-wired, in-office systems, are increasingly on the move too.

Breaches are costly any way you look at it. At minimum, the public loses confidence. Often, data falls into criminal hands. Sometimes, there's international political fallout. And at the upper end, the consequences can be a matter of national security.

For these reasons, regulations around data storage and transmission continue to evolve and affect the workings of most government departments.

## Staying Current with Compliance: Why it's so Challenging

In the US, the story is already complex, and increasingly so. And the more regulations shift, the tougher it is for government organizations to keep up. An InformationWeek.com survey found that, of government respondents, "nearly 60% say their mobile data protection policies are driven by both internal prioritization and federal and state requirements. However, technical controls to support policies are not always in place. For example, just 27% can prevent data from leaving secured devices."<sup>1</sup>

**In Canada, departments must navigate a range of federal policy instruments and recommendations on security, including these:**

- Policy on Government Security
- Directive on Departmental Security Management
- Operational Security Standard: Management of Information Technology Security (MITS)
- Information Technology Security Guidance 33
- Communications Security Establishment Canada: Top 35 Mitigation Measures

**Other legislation impacts how wireless networks and devices are deployed for privacy, employee behavior, and government asset management, including the:**

- Public Service Labour Relations Act
- Public Servants Disclosure Protection Act
- Public Service Employment Act
- Security of Information Act

Lastly, policies in other areas impact mobile device usage, such as the:

- Policy on Conflict of Interest and Post-Employment
- Policy on Information Management
- Policy on Legal Assistance and Indemnification
- Policy on Management of Information Technology
- Policy on the Management of Materiel
- Policy on Privacy Protection

## Are Government Agencies More Secure Than Private Sector Enterprises?

According to a recent US survey<sup>2</sup> of government employees:

- On mobile devices, 31% use a public Wi-Fi connection, but 25% do not set passwords.
- 6% of government employees who use a mobile device for work say they've lost or misplaced their phone. In the average Federal agency, that's more than 3,500 chances for a security breach.
- Despite the Federal Digital Government Strategy, more than 25% of government employees have not received mobile security training from their agencies.
- In Canada, federal departments report thousands of data, information or privacy breaches each year. But the worst offender was the Canada Revenue Agency, where breaches impacted 2,249 people.<sup>3</sup>

### Governments Today Need Comprehensive Mobility Management Solutions That

- Provide single-console mobility management for devices, applications, network access, security and controls
- Allow them to create, deploy and manage powerful cross-platform applications
- Ensure a high level of data encryption, both in-transit and at rest on mobile devices
- Monitor, detect and create alarms and actions based on unauthorized access or usage
- Provide the capability to log various mobility network data and voice traffic, such as PIN, SMS, phone, and BBM™ messages
- Provide flexibility to adapt as needs change over time
- Are scalable to address new needs and growth requirements
- Are easy to implement and manage, and are designed to enable operational efficiencies
- Include the support they need, customized to their unique requirements, from the planning and installation phases through to daily operations

In an effort to take steps to “improve the quality of Government services to the American people,” the “Digital Government Strategy” was released. Soon afterward, the Federal CIO Council chartered an investigation to “evaluate opportunities to accelerate the secure adoption of mobile technologies into the Federal environment at reduced cost.”<sup>4</sup> The study identified the following near-term requirements.

### Mobile Device Management

Improvements in tools and processes are necessary to support enterprise-level configuration management and controls for Federal agencies.

## Identity Access Management

The use of the Personal Identity Verification (PIV) standard for user authentication is not well supported by existing products. Implementation of FIPS 201-2 and NIST SP 800-157 will require focused attention to ensure proper implementation and market support for user authentication tools.

## Application Services

Better tools and processes are needed to accredit and distribute applications required for Government missions, leveraging commercial market cycles, and commercial and Federal application stores.

## Improved Governance and Standards

The Federal Government must work collaboratively with the industry to bridge the security gaps present in today's smartphones, tablets, and other mobile devices, while continuing to identify policy and legal issues that may need to be addressed to accommodate these new technologies and better fulfill agency mission requirements.

## What to Include in Your RFP/RFQ to UEM Vendors

**If you work for a governmental organization and you're part of a team evaluating Unified Endpoint Management (UEM) solutions, you need to know that the solution you choose will:**

- Allow you to mobilize tools, processes and people in a way that helps you deliver on all your organizational goals and mandates
- Give you the flexibility to meet your compliance requirements, anywhere and everywhere, even as those needs change over time
- Support and integrate with additional mobility value-added services that your organization may require – if not today, in the near future

Chances are, you're developing a detailed RFQ (Request for Quotation) or RFP (Request for Proposal) document that asks each vendor to address very specific questions on a host of topics, many of which will relate to compliance and to security in general.

Assembling this document can cost a lot in terms of time and resources. If you haven't done it yet, here's a sample of the kind of detail you'll want to include. Although based on real questions that government organizations have included in their RFPs/RFQs, this list is by no means exhaustive. Rather, it will give you an idea of the type of questions you should ask UEM vendors during your vetting process to determine whether their platform can help you address the relevant regulatory, privacy and security requirements.

Because it's focused on compliance-related topics, this list does not cover other important UEM factors that should be part of your RFP – for example, questions related to implementation, integration with other enterprise mobility services, tech support, devices supported, etc. For support in assembling a full RFP or RFQ, reach out to your BlackBerry® contact, who will be happy to help.

**Choosing the right UEM solution means ticking hundreds of boxes. But there are some broad must-haves that make good business sense for every government organization, regardless of size or location.**

## **Data Leakage Prevention (DLP)**

**Q:** How does the UEM solution separate work and personal applications and app data?

**Q:** How does the UEM solution ensure that data can't be 'leaked' between secure enterprise applications and personal applications?

**Q:** Does the UEM solution allow us to restrict clipboard copy and paste operations? Can we ensure copy and paste happens only between protected and authorized mobile apps?

**Q:** Does the UEM solution allow us to prevent mobile app data from being copied during device or cloud backups?

**Q:** Does the UEM solution provide a way to control/ restrict the transfer of data from a mobile device to a desktop/laptop when connected or tethered?

**Q:** Does the UEM solution allow us to disable the screen-shot feature on a mobile device?  
Does this differ by operating system?

## **Encryption**

**Q:** Does the UEM solution provide encryption for both data at rest and data in transit? If yes, what type of encryption?

**Q:** What level of encryption does the UEM solution provide to separate work application and personal application data on a mobile device?

**Q:** Does the UEM solution enable FIPS 140-2-compliant cryptography? If yes, does it provide Level 1 or higher?

**Q:** Are encryption keys, initialization vectors (IV), and static salts randomly generated?

**Q:** Can the UEM solution be used to manage encrypted Enterprise Instant Messaging (EIM) services?  
To what extent?

## **User Privacy**

**Q:** Can a device be remotely locked if we suspect it has been lost or left in an unsecure location?

**Q:** Can all data on a mobile device be wiped if it is lost or stolen? Does the UEM solution have the ability to selectively wipe only work data from the device, leaving the personal information intact?

**Q:** Does the use of location tracking functionality require explicit opt-in from the end user?

**Q:** Does the UEM solution verify a user's identity prior to resetting a password to prevent both unauthorized access to personal information and hacking attempts via social engineering?

**Q:** Can the UEM solution be configured to allow a device to automatically wipe itself after a certain number of incorrect authentication attempts?

## **Access to Cloud-Based Services**

**Q:** Does the UEM solution allow us to restrict document and file sharing via iTunes (iOS)?

**Q:** Does the UEM solution allow us to restrict iCloud and other cloud services for document and file sharing?

**Q:** Does the UEM solution support Microsoft® Office 365™ users?

## **Identification and Registration**

**Q:** Does the UEM solution offer self-service options for all employees? What features are available?

**Q:** Does the UEM solution operate in real time (so that users can be added or deleted immediately)?

**Q:** Does the UEM solution have the ability to track and restrict authorization and authentication for multiple logins on the same device (if the device is authenticated only for a set of predetermined/preidentified users)?

**Q:** Does the UEM solution integrate with enterprise solutions for Identity & Access Management (IAM), and in particular, for cloud-based IDs? To what extent?

## **Mobile Applications Security**

**Q:** Can we prevent user groups from installing certain mobile apps, and make other apps mandatory for particular groups?

**Q:** Does the UEM solution store credentials and configurations in encrypted form independent of the device?

**Q:** For sufficient post-event auditing: can all device and environmental attributes, including GPS coordinates, be exposed to applications and logging?

**Q:** Can we prevent mobile applications from trusting any client-side authentication or authorization tokens?

**Q:** Does the UEM solution have control over links within email, with the ability to force links to open in a secure native browser where required?

**Q:** Does the UEM solution enable users to open an attachment, update documents using secure editors, and send without leaving the secure container architecture?

**Q:** Can we use the UEM solution to set content download restrictions (e.g. for roaming)?

**Q:** Can we enable granular app controls to blacklist undesired apps and control VPN access per app?

## **Software and Policy Updates**

**Q:** Does the UEM solution have the ability to auto- update applications remotely?

**Q:** Does the UEM solution allow us to enforce a check for policy and app updates as often as we choose?

**Q:** Does the UEM solution allow us to force an upgrade to a new mobile app version after a configurable amount of time has elapsed?

**Q:** Does the UEM solution provide the ability to maintain an audit trail of all updates (e.g. OS, app installation, app versions) to a device?

**Q:** Does the Enterprise App Store notify users about available updates?

## **Certificates**

**Q:** Does the UEM solution have the capability to deploy a certificate, as well as a provisioning profile, for each application deployed to an end user?

**Q:** Are all digital certificates kept current, issued by a well-known certificate authority, and associated with the correct hostname?

**Q:** Are encryption keys protected during transit and in storage? Is access to encryption keys restricted to authorized personnel?

## **Containerization**

**Q:** Can the UEM solution enable a full container mode for work apps and data?

**Q:** In corporate-liable scenarios, does the administrator (optionally) have full control over all applications on the device, including corporate and public applications, whether they're made optional or mandatory?

**Q:** Can the UEM solution restrict document and file sharing between mobile apps on the same device?

**Q:** What methods of authentication are provided to enable container authentication?

**Q:** Is the solution able to leverage those authentication types across apps? How so?

## **Reporting**

**Q:** Does the UEM solution allow us to log and report on configuration, deployment, use and the availability of business data/applications on devices? Is this information made available via Microsoft® Excel® or other formats that can be manipulated?

**Q:** Can all mobile device data traffic be captured, including chat (IM), texting (SMS) email and phone numbers (dialed and received)?

**Q:** Does the UEM solution produce sufficient logs and/audit trails to support the investigation and forensic analysis of security incidents?

## **Network Management and Security Event Logging**

**Q:** Does the UEM solution have the capability to log various mobility network data and voice traffic, such as PIN, SMS, phone, and BBM messages (chats, video calls)?

**Q:** Can all IT commands and application deployments/wipes be logged?

**Q:** Describe what the UEM solution requires from an external-facing firewall/security perspective.

**Q:** Does the UEM solution fully support Active Directory? Can configurations be assigned to users via AD groups?

**Q:** Do all log entries include the following attributes?:

- The time and date of the event
- The application associated with the event
- The user or process initiating the event and, if applicable, the subject acted upon
- The remote IP address of the initiating user or process
- Success or failure indication
- A detailed description of the event

**Q:** Can the UEM solution enforce policies based on the geographic location of the device?

**Q:** Does the UEM solution enable advanced gatekeeping to control access to Microsoft® Exchange ActiveSync by device?

**Q:** How many ports are required? (Single outbound port consolidation simplifies IT management while reducing the threat posed by malicious attacks)

**Q:** Can the UEM solution allow us to route all traffic through the corporate infrastructure?

**Q:** Please describe the UEM solution's system health diagnostics capabilities in detail.

## **Mobile Device Usage Policies**

**Q:** How does the UEM solution maintain device usage policies that are applied to a profile on the device?

**Q:** Does the UEM solution have the ability to push updated policies to a profile on the device?

**Q:** Can the UEM solution validate that updated policies have been applied?

**Q:** Can the UEM solution be used to set user profiles for activation, SSO and proxy settings?

**Q:** Can it be used to limit the number and type of devices, and easily manage multiple devices per user?

**Q:** Can we set policy and device controls based on device ownership model (COPE, BYOD etc.)?

## **Passwords**

**Q:** Can the UEM solution force users to change their passwords upon first login with an initial password or a reset password?

**Q:** Does the UEM solution encrypt authentication credentials in transmission and in storage?

**Q:** Can the UEM solution force password changes, force the use of multiple character types in password creation, and restrict the use of previous passwords? Does it allow us to restrict device use and/or wipe data after a set number of unsuccessful login attempts, and lock the device after a set time of non-use?

**Q:** Where are the user IDs and passwords stored for validating user credentials? How are they protected (i.e. encrypted or hashed)? If a password is hashed, is a user-specific salt used?



## **Mixed Security Requirements**

**Q:** Does the UEM solution easily support all device ownership and management models such as bring your own device (BYOD), corporate-owned, personally enabled (COPE), corporate-owned, business only (COBO), choose your own device (CYOD), etc.?

**Q:** Does the UEM solution allow a mix of security and access policies for roles with varying sensitivities and security requirements? (e.g. employees/ partners/contractors)

**Q:** Does the UEM solution allow for differing policies and user capabilities based on groups or departments?

## **Jailbreaking/Rooting**

**Q:** Can the UEM solution detect jailbreaking/rooting on iOS and Android™ devices? Can it be configured to take various actions including wiping the work container or the entire device when the device is out of compliance?

**Q:** Does the UEM solution detect when a user tries to tamper with client components, jailbreak or root the device, or uninstall clients/profiles?

**Q:** Can access to enterprise systems be limited/ denied based on the device's operating system version (including whether the device has been rooted/jailbroken) or its mobile device management software client version (if applicable)?

**Compliance remains a constant challenge for government agencies as their mobile ecosystem broadens and employees expect to work from anywhere as if they were sitting at their desk in the office.**

## How BlackBerry Ticks All the Boxes for Government Organizations

BlackBerry® Unified Endpoint Manager (UEM) provides the control and visibility IT needs with the flexibility to support all your endpoints, ownership models and use cases.

BlackBerry UEM is a part of the BlackBerry Enterprise Mobility Suite, offering a trusted end-to-end approach to security, and allowing organizations to support a wide range of endpoints, including iOS®, Android™, Android™ for Work, Samsung Knox™, Windows®, macOS and BlackBerry®.

BlackBerry security is trusted by thousands of enterprises around the world to lock down mission-critical data. With 70+ security certifications, more than any other mobile vendor, BlackBerry meets compliance requirements for organizations in even the most strictly regulated industries.

BlackBerry UEM provides a secure, end-to-end, behind-the-firewall outbound-initiated connection integrated into the device workspace. VPN-less secure connectivity can be set for the whole device, container or specific apps, which require access to behind the firewall resources. With BlackBerry UEM, your mobile traffic travels over the secure BlackBerry network to ensure data security, protecting your most important asset — your business data.

## Staying Current with Compliance: Why it's so Challenging

As your mobile needs evolve, BlackBerry UEM can grow with them. From secure mobile collaboration to mobile content to a wide range of secure mobile apps, BlackBerry UEM and the BlackBerry Enterprise Mobility Suite ensure you can deploy additional mobile capabilities as you need them without time-consuming and costly rip-and-replace migrations.

Choosing a single solution for your endpoint management requirements can help your organization standardize infrastructure, reduce complexity and increase ROI. Both deployment options for BlackBerry UEM—cloud and on-premise—are cost-effective and flexible so that you can scale up or down as your needs change. User-based licensing enables management of many endpoints, on any platform and with any ownership model.

Talk to us to find out how BlackBerry can address every one of the issues on this checklist.

In the meantime, visit [blackberry.com/suite](http://blackberry.com/suite) to learn more about our mobility management solutions, and get started with a free trial of the BlackBerry Enterprise Mobility Suite that's right for your organization.

## About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols “BB” on the Toronto Stock Exchange and “BBRY” on the NASDAQ. For more information, visit [www.blackberry.com](http://www.blackberry.com)