



KNet MaaS for Public Sector

Powered by Fiberlink's MaaS360®



KNet MaaS in Action: Avoid the Mobile Cliff

Do you worry when a government worker downloads sensitive documents to their mobile device and then loses the device? Don't. KNet MaaS has you covered. With KNet MaaS, the employee can take immediate action, going to a self-service website, locating their device and, if necessary, locking it to prevent access.

If the device cannot be recovered, then the employee or IT administrator can fully or selectively wipe it to protect your agency's sensitive emails, documents and apps. In addition, KNet MaaS enables you to create policies to turn off the camera on a mobile device when it enters a secure area, set different security policies based on the encryption levels of Wi-Fi connections, and control access to downloadable encrypted documents on a per group or per user basis.

Challenges for the Public Sector

The exploding use of mobile devices by government workers challenges IT departments at federal, state and local levels. According to recent surveys, most government IT professionals say they lack the necessary tools to manage mobile devices effectively.

Employees want specific devices—increasingly, personally-owned devices—to maximize their job performance and productivity. The drain on IT resources to support all mobile platforms can be overwhelming—and expensive. And efforts can still fall short of your agency's information security and compliance policies.

IT directors need an efficient way to manage devices while still meeting unique security requirements such as the Federal Information Security Management Act (FISMA), which now includes continuous security monitoring and monthly reporting, and Federal Information Processing Standard Publication 140-2 (FIPS140-2) compliance.

FISMA

Fastest Time-to-Solve Your Challenges

KNet MaaS—the first and only cloud-based, FISMA-certified MDM solution—gives you the fastest time-to-solve your mobile security challenges in the industry by enabling federal, state and local governments to safely embrace workforce mobility trends with a robust and mature platform for controlling security and compliance on all agency and employee devices.

Using KNet MaaS, Mobile Device Management (MDM), Mobile Application Management (MAM), and secure document and expense management can easily and instantly help agencies conform to government initiatives for Telework, Green IT, Continuity of Operations (COOP), Continuous Monitoring and Cloud First.

Key Benefits

- Gain 360° visibility and control of all mobile devices, apps, documents and files
- Automate password, encryption and policy enforcement
- Ensure anytime, anywhere device and data security with immediate remote action on nonconforming devices
- No infrastructure changes required
- Rapid implementation
- Low implementation costs and no-fuss maintenance
- Expense management to control costs

Key Features

- Supports today's mobile devices from a single console, including iPhone, iPad, Android, Windows Phone, BlackBerry and Kindle Fire
- Instant device enrollment via SMS, email or URL over-the-air (OTA)
- Pushed policies, encryption and security safeguards
- Contextual, event-based policy, security and compliance rules engine enabling automated actions for non-compliance
- Enforce usage policies specific to departments or teams
- Remote locate, buzz, lock and wipe (full and selective) device
- Blacklisting, whitelisting and requiring apps
- Customized agency app catalog
- Control document distribution (including restricting forwarding) and versioning
- Real-time reporting and analytics



KNet MaaS for Public Sector

Control All Devices

KNet MaaS gives government agencies coordinated visibility and control over all devices and operating systems, from Apple iOS to Android, Windows Phone and BlackBerry. Integrated dashboards, analytics and reporting provide actionable intelligence to government IT departments about their entire mobile environment through a single console. IT administrators can quickly visualize the distribution of devices, apps and documents across platforms, ownership, compliance status and more to control workforce mobility risks.

Improve Mobile Information Security and FISMA Compliance

KNet MaaS provides the ability to know and control information security safeguards on all mobile devices and react rapidly to lost or stolen devices with the only MDM cloud service to receive authority to operate (ATO) under FISMA. As part of the certification process, Fiberlink included the FedRAMP controls, which are designed specifically for cloud providers, and also fully supports requirements for CyberScope reporting. Government IT departments can:

- Push policies and Wi-Fi, email and VPN profiles OTA
- Quarantine new devices automatically until authorized to access your network
- Enforce passcode protection, encryption, security updates and continuous monitoring in accordance with FISMA 2.0
- Remotely locate, block or wipe (full and selective) devices lost, stolen or no longer authorized
- Blacklist applications and block device access

Control Mobile Applications

KNet MaaS application management allows government agencies to easily manage and secure the applications that are critical to your users. An on-device app provides users with a catalog of authorized agency and public apps. Users can view the apps made available to them, install apps, and be alerted to updates. IT and other departments can manage the master app catalog and per-user authorization. App lifecycle management provides real-time software inventory reports, app distribution and installation tracking, update publishing, provisioning profile management, and app security and compliance management.

Reduce IT Workload and Costs

With KNet MaaS' 100% cloud-based platform, there are no servers to install, no complex configurations or infrastructure changes, and no investment in expensive software. Built on a secure, multi-tenant cloud architecture, KNet MaaS enables instant mobility management in just minutes with effortless scalability, whether from ten to tens of thousands of users, and seamless integration into existing backend systems to help agencies conform to government initiatives for Telework, Green IT, Continuity of Operations (COOP), Continuous Monitoring and Cloud First. Additionally, KNet MaaS eliminates the strain and expense that rapidly changing mobile devices and apps can have on IT organizations by automatically incorporating the continuous stream of platform updates.

Why KNet MaaS?

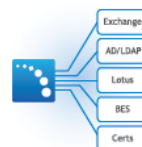
Federal, state, and local government customers trust KNet MaaS to manage and secure their devices, apps and documents, including the Department of Interior, Department of Commerce, and General Services Administration (GSA). KNet MaaS is available for government agencies to purchase through the GSA Schedule 70, SEWP and other contract vehicles.



**Proven approach
to cloud-
based mobility
management**



**Powerful
management
& security to
address the full
mobility lifecycle**



**Seamlessly
integrates
with all of
your existing
infrastructure**



**Simple &
fast with an
exceptional
customer
experience**

For More Information

To learn more about our technology and services visit www.knet.com.au.

104 Byng St, Orange NSW 2800

Phone +61 2 6363 8999 | Fax +61 6363 1500 | sales@knet.com.au