OIG
In Your Inbox

Insights, Advisories and Alerts

Vol. 1, Issue 3 | August 2025

Strategies to Manage Mobile Devices

Introduction

In many workplaces, mobile devices are integral to employee productivity. Thoughtful policies concerning office-issued mobile devices are an important tool for the prevention of waste and abuse of office resources. Equally important are written procedures to collect devices and terminate lines for departed employees to prevent unauthorized use and additional charges. Regularly reviewing and updating your office's policies and procedures is also critical to the successful mitigation of the risks around the use of these devices in the public space.

Everyone is connected, so what's the problem?

If you issue mobile devices without considering whether an employee's role or responsibilities require their use, you risk creating the impression that the office-issued mobile device is a perk intended to supplant an individual's personal device. In addition to blurring the line between personal and official use, this practice leaves you exposed to costly charges for services unrelated to work, such as international calling, text, or data. In some cases, office resource policies can leave you, the employer, responsible for the cost (or replacement cost) of a lost or damaged device.

Employers often fail to think about selecting data plans for consistency with organizational needs. Wireless carriers use data plan names that are unrelated to the specific components of the plan. For example, one major U.S. wireless carrier offers plans such as "Unlimited Ultimate," "Unlimited Plus," and "Unlimited Welcome." Look at the components of each plan, and the costs of those components, to align with your organizational needs, rather than simply selecting from plan names that sound similar. For example, while including unlimited texts in your plan may make sense to further your business purposes, unlimited streaming may be an unnecessary component.

After the initial purchase, data plans can seem as if they are on autopilot. Bills come in and are paid without much scrutiny. This mindset makes it particularly easy to become lax about reevaluating the use of these resources, especially if the bills are small relative to your overall budget. How an agency manages one public dollar is indicative of how it manages $1 million.

Incomplete policies and inconsistent monitoring of the assignment and use of office-issued mobile devices can also lead to data security risks from devices that have access to your systems. As part of your enterprise-wide data security strategy, you need to have policies and procedures for terminating lines and retrieving devices when an employee departs.

Recommendations

The OIG works alongside all recipients of public resources to mitigate risks, provide good stewardship, and reduce wasteful spending. The best practices recommended below go a long way in preventing unnecessary device and data expenditures while maintaining operational efficiency:

A. Know your operational needs when choosing a plan.

1. Critically consider whether an office-issued mobile device is required for individual roles. If so, what type of device is most appropriate? Different roles may require different functionalities.

2. Review the details of your data plan. If there are multiple data plans, consider whether the plans can be standardized in any way. Stay informed about changes to plan details and costs. Leverage government contracts and discounts to get better rates on the services you need.

B. Lead with policy.

1. Whether simple or complex, any policy surrounding office-issued mobile devices should answer these questions:

   a. Who is entitled to receive an office-issued mobile device? Why?

   b. What is an appropriate and acceptable use of an office-issued mobile device? What requirements will you place on employees in exchange for their acceptance of an office-issued mobile device?

   c. How will you handle loss, theft, or unexpected charges?

   d. How will you monitor compliance with office policies?

   e. What steps can you take to protect office data?

   f. Can you retrieve office data from the mobile device for record retention purposes?

   g. Does your policy clearly state that an office-issued mobile device should not serve as a replacement for an employee's personal device?

   h. Is incidental personal use allowed?

2. Your policy won't cover every single scenario that comes up. When you depart from the policy, document the exemption and include the reasoning for the departure.

3. Issue periodic reminders to keep employees aware of their responsibilities.

C. Conduct regular and frequent reviews and reconciliations.

1. Bills can increase quickly, sometimes within a single billing period. Review charges on a monthly basis, focusing on:

   a. Regular monthly charges;

   b. Additional charges for the billing period; and

   c. Usage details (data, text, and calls).

Conclusion

Understanding your operational needs for mobile devices, adopting policies to govern their use, and regularly evaluating monthly charges will help ensure optimal use of these resources. This recommended three-pronged approach will assist you in identifying the mobile tools and procedures needed to effectively fulfill your public duties and will also support your role as a steward of public assets.

*The OIG periodically issues **OIG In Your Inbox: Insights, Advisories and Alerts** as a way to succinctly share timely topics with key stakeholders, most notably the leaders within the Commonwealth's 351 local communities. The OIG hopes that **OIG In Your Inbox: Insights, Advisories and Alerts** will prompt dialogue and needed action on matters important to public entities.*

Massachusetts Office of the Inspector General

Visit Us At
www.mass.gov/ig

Connect With Us At