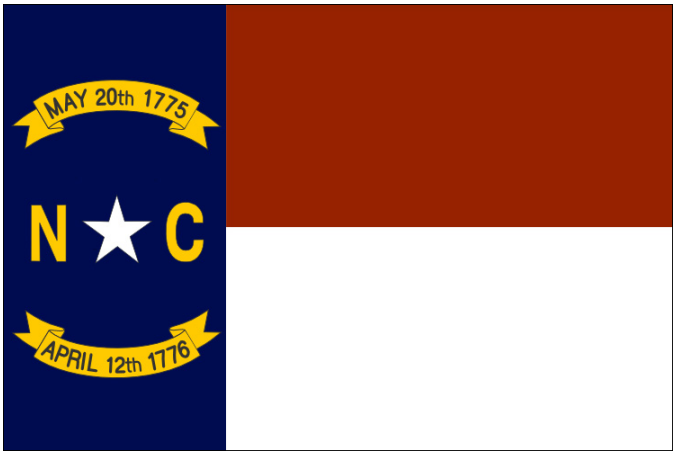
Developing a Policy for Bring Your Own Device



Report to the Joint Legislative Oversight Committee on Information Technology

Chris Estes

State Chief Information Officer

Office of Information Technology

September 2013

This page left blank intentionally

Contents

This page left blank intentionally

Legislative Request

SECTION 7.18.(d) of Session Law 2013-360 directs the Office of the State CIO to develop a policy for implementing a "bring your own device" plan for State employees. By September 1, 2013, the State CIO shall report to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on how the plan is to be implemented, as well as on potential issues and costs. Following consultation with the Joint Legislative Oversight Committee on Information Technology, the State CIO may implement the "bring your own device" plan.

Report Focus

1. Develop a Policy for implementing BYOD plan (Policy Considerations)
2. How the policy plan is to be implemented (Roadmap)
3. Potential policy issues and cost
4. Consultation for implementing BYOD plan (Next Steps)

Introduction

We live in a mobile society, with an always-on workforce that expects to be constantly connected to work and home. This presents multiple challenges to employers in both the public and private sectors as they try to balance business interests with their employees' desires. Nowhere is this balancing act more pronounced than the technology used in the workplace. Today's employees bring an expectation that they can use their personal laptop, tablet or smartphone for work.

State government is no different. State employees, like those in the private sector, already use their personal devices in the workplace. Some agencies pay employees a stipend for using their own smartphones.

Statewide policies regarding security, public records and confidentiality apply to government documents and data stored on personal devices, but no statewide policy specifically addresses the use of mobile devices. Agencies can determine the types of devices their employees use, the amounts they are reimbursed, and the security controls—if any—that are deployed. This approach needs to be fixed, given trends in the marketplace and citizens' growing concerns over the security of their data.

The management of mobile devices is only one component of a much larger shift in the technology industry. Enterprises are moving away from technology solutions and operations are designed and

developed based on the requirements of specific **devices** (e.g. desktop/laptop pc's; mobile phones, server systems).

Modern trends are moving towards a **user-centric** approach. In that model, solutions are designed around the user's needs and a workspace can follow a worker across their mix of devices and locations. North Carolina IT is moving in this direction and a "bring your own device" (BYOD) policy is one consideration in support of this transformation.

This report summarizes some of the policy considerations and outlines an approach for developing a BYOD Policy for North Carolina state government. The State CIO is providing the report to the Joint Legislative Oversight Committee on Information Technology pursuant to Sect. 7.18(d) of Session Law 2013-360, which is included in the Appendix.

Policy Considerations

Any BYOD policy must address a number of interconnected issues. Basically, they can be divided into four three areas: devices, security, cost and reimbursement.

Devices

A threshold question in the development of any BYOD plan is what devices will be allowed? Will state employees be allowed to bring any type of device into the workplace, whether it's a smartphone, a tablet, a laptop, or a wearable device, such as Google Glass? If so, are there any limits on the operating systems? Are they limited to systems that are compatible with the enterprise, so that employees can read and edit documents, for example? If the devices are not compatible, who is responsible for supplying the necessary software: the employee or the state?

Support for devices is another consideration. Are employees on their own when their device will not connect to the network, or they cannot use the email system? Or will the help desk handle those issues, which increases cost and complexity?

Security

Citizens are increasingly concerned about their privacy and the billions of bits of information about them stored by government and businesses. The proliferation of personal devices in the workplace makes protecting citizen data even more difficult for IT security professionals. Every PC, smartphone, desktop, and tablet on the network is a pathway for hackers and their malicious software, and a potential source of data loss if the device is lost, stolen or hacked.

Security policy considerations must flow from a decision on the approach the state will use, specifically whether it will invest in a centralized mobile device management system, or manage controls at the agency or device level. Authentication of devices to ensure that state employees are using them, not hackers, is another baseline issue. The state could adopt a system allowing different levels of access, depending on the device.

Once the framework is established, policies dealing with specific risks and incidents must be developed. For example, should the state have the authority to wipe all data on a personal device that is lost or stolen if the state documents are not isolated? If so, that authority should be clearly spelled out for employees.

In establishing security policies, the state must also balance employees' desires to keep their personal information private with state laws regarding public records. In North Carolina, public records are public no matter where they are located, and employees must fully understand that when bringing their own devices to the workplace. Along the same lines, employees must be fully informed that state laws and rules dealing with disposal of records apply to state documents on their personal devices.

Policies alone are only as good as employees' willingness to follow them, and to practice safe computing skills

Cost

Technical controls and a centralized management system would increase security, but also increase costs. Even marginal costs of a few dollars per month per device would significantly impact any business case.

Reimbursement

As mentioned previously, many agencies already provide a stipend for employees to use their personal devices for work. The Office of State Budget and Management (OSBM) has established broad guidelines for the reimbursement, but agencies set their own policies as to who is eligible, and the amount of the stipend. A statewide approach would provide equity to the system and make administration easier.

Roadmap

Tackling these and other issues, while collaborating with all of those affected, is a complex task. But given the usage of personal devices today, there is no time to wait for a comprehensive plan. We

propose a series of steps that will lead to a sound, easily understood, secure and flexible plan for the use of personal devices in state government. This will be done in three steps.

Short term

By January 1, 2014, the State CIO will adopt an interim policy on the use of personal devices in state government. At a minimum, the policy will:

- Allow the use of personal devices by state employees to conduct state business
- Set minimum standards and guidelines for their use
- Make it clear that users of personal devices that are being used to conduct state business must comply with state laws and rules dealing with public records, records retention and confidentiality
- Allow agencies to determine reimbursement rates and rules, consistent with the OSBM guidelines.

Middle term

The State CIO will develop a broader plan and policies for BYOD across state government, expanding the security and compliance approach. This will be completed by May 1, 2014, and presented to the Joint Legislative Committee on Information Technology Oversight, pursuant to the budget bill. With approval from the committee, the State CIO will begin implementing the plan.

Long term

ITS will implement a more comprehensive BYOD plan, including any procurement, and begin planning for the future to align the plan with the state's overall end-user strategy.

Issues & Cost

The following bullets summarize some of the primary challenges with a BYOD policy that need to be understood:

- Types of devices that will be permitted on the state's network
- Types of users that will be eligible to participate in a BYOD program
- Prohibiting confidential business information residing on endpoints or only in isolated, encrypted form, and only when absolutely necessary

- Management of the endpoints including full or selective remote wiping of a device on the state's network
- Support expectations for personally-owned devices and state services
- Should a subsidy or stipend be provided for personally-owned devices and other services as the state moves towards a user centered end user computing environment
- Additional costs associated with hardware and software required to enable productive use of personal devices while ensuring necessary security and compliance controls
- Potential for cost savings associated with:
    - modified support levels offered for personal devices thereby reducing support staff requirements
    - savings associated with providing a fixed stipend for the purchase of personal devices instead of State procurement of a computer system
- Clear definition of device, applications and data ownership
- Integration of BYOD with the mobile device policy

Next Steps

The following actions will be taken to inform and create the strategy for the short and middle term roadmaps:

- Implement currently available capabilities to better secure mobile devices on the state network
- Work across agencies to determine BYOD needs and requirements to create enterprise level view
- Identify persona types for personal devices that would participate in a BYOD program and scenarios where it is inappropriate due to data security, worker type or other factors
- Determine how virtualization impacts a BYOD policy as the state moves to a user centered computing environment
- Work with other states and private sector partners that have implemented a BYOD policy for guidance and best practices
- Work with OSBM to understand how cost considerations of a BYOD policy that would include other endpoints such as laptops and desktops
- Investigate mobile device management solutions and support infrastructure for testing to securely manage endpoints

Appendix

Section 7.18, Session Law 2013-360

USE OF MOBILE COMMUNICATIONS DEVICES

SECTION 7.18.(a) By October 1, 2013, every State agency shall submit to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division a copy of the agency policy on the use of mobile communications devices. This reporting requirement is continuous such that any time a change is made to an existing policy, the agency shall submit an update immediately.

SECTION 7.18.(b) Beginning October 1, 2013, each State agency shall submit a quarterly report to the Joint Legislative Oversight Committee on Information Technology, the Fiscal Research Division, and the Office of the State Chief Information Officer (CIO) on the use of mobile electronic communications devices within the agency. The report shall include the following information:

(1) The total number of devices issued by the agency.

(2) The total cost of mobile devices issued by the agency.

(3) The number and cost of new devices issued since the last report.

(4) The contracts used to obtain the devices.

SECTION 7.18.(c) The Office of the State Chief Information Officer shall review current enterprise, and any individual agency mobile electronic communications contracts, to develop a plan to consolidate the contracts. By October 1, 2013, the Office of the State CIO shall submit a report on progress toward consolidating State agency mobile communications device contracts to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

SECTION 7.18.(d) The Office of the State CIO shall develop a policy for implementing a "bring your own device" plan for State employees. By September 1, 2013, the State CIO shall report to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on how the plan is to be implemented, as well as on potential issues and costs. Following consultation with the Joint Legislative Oversight Committee on Information Technology, the State CIO may implement the "bring your own device" plan.