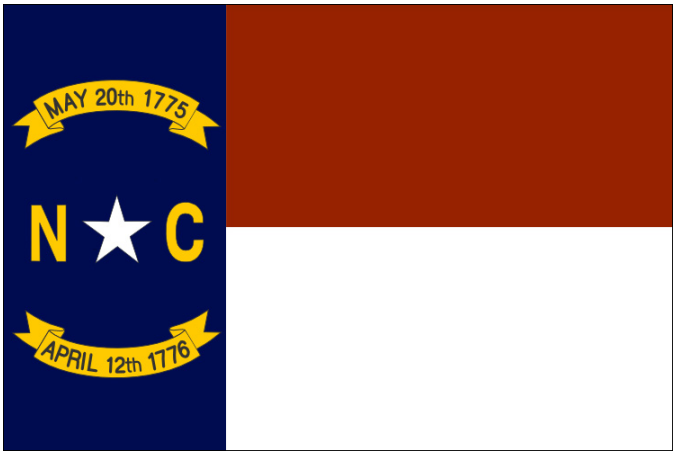
Bring Your Own Device Policy



Report to the Joint Legislative Oversight Committee on Information Technology

Chris Estes
State Chief Information Officer
Office of Information Technology
March 2014

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 Chief Information Officer (CIO) to develop a policy for implementing a "bring your own device" (BYOD) plan for state employees. The full text of the legislation is in Appendix A.

In response to the legislation, the State CIO in September 2013 presented a report entitled *Developing a Policy for Bring Your Own Device* to the Joint Legislative Oversight Committee on Information Technology. The plan outlined a three-stage approach, with an interim policy in place by January 1, 2014. At minimum, the interim policy would:

- 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.

Report Focus

This report outlines current state policies regarding use of mobile devices, and for reimbursing employees who use their own device to conduct state business. With minor, clarifying changes, these provide acceptable interim standards.

A roadmap for development of a comprehensive end-user strategy that would address all devices used by state employees to conduct state business is also discussed. The new strategy will shift the focus of information security from devices to the data, no matter where it is stored.

Introduction

As noted in the September 2013 report, we live in an increasingly mobile society. Today's workers expect to use their personal devices, such as smart phones and tablets, for both work and their personal lives.

A report by the Federal Communications system in March 2013 underscored the dramatic increase in the use of mobile devices. Citing industry data, it said mobile data traffic in the United States increased 62 percent from 2011 to 2012, and the traffic in 2012 was about 73 times the volume of traffic in 2007. The report projected that the amount of data in 2017 will be nine times the volume in 2012.The explosion of mobile device use presents challenges for IT management in both the public and private sector.

State government has recognized this challenge by adopting policies that allow state employees to use personally owned devices to conduct state business, and to receive reimbursement for use of their devices. The *Statewide Information Security Manual*, adopted by the State CIO, provides standards for use of mobile devices, including those owned by individuals. The *North Carolina Budget Manual* includes policies for reimbursing state employees who use their personal devices to conduct state business. A number of agencies have adopted their own policies that conform to the statewide standards.

Policy Considerations

To begin developing a BYOD policy, State CIO's staff reviewed the current requirements for using mobile devices in the *Statewide Information Security Manual,* which applies to Executive Branch agencies, excluding the university system. Section 050406 sets security standards for all mobile devices that are used to conduct state business, whether the devices are owned by the state or employees.

The existing standards provide a minimum level of protection. Short- and long-term efforts are under way to strengthen the protection of citizen data.

In the short term, the State CIO's office is revising current standards to require encryption for personally identifiable and confidential information on all mobile devices, not just those supplied by the state. The change would not require employees to encrypt their phones. The requirement would apply only if the employees had personally identifiable information on the device.

Another clarification would make it clear that agencies must follow State Budget Manual guidelines for reimbursing employees for use of their personal devices.

Over the longer term, the State CIO's staff is developing a comprehensive end-user strategy that will apply to all types of devices used by state employees to conduct business. Current policies focus on protecting data at the device level, whether that is a smartphone or a server, by building walls around the device. Over the long term, the State CIO's office is shifting the overall emphasis on security to protecting data, no matter where it resides. Industry standard approaches to maintaining security across user endpoints are mobile device management (MDM) and virtualization solutions.

MDM solutions manage applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablets. This solution can apply to both state-owned and employee-owned (BYOD) devices across the enterprise. MDM solutions provide a means to secure work email and data by isolating work applications and data from personal applications and data. In addition, if a device is compromised or lost, a MDM solution can restrict access to sensitive data and even erase everything on the device if necessary.

Application and desktop virtualization solutions provide authenticated access to a user's applications and data from any computing device, from desktops and laptops, to any mobile device. The applications do not run locally and data is not stored locally on the computing device. Both applications and data are physically located on a secure server in a data center. The user only accesses their

applications and information through a secure connection from the computing device to the data center server. The user's personal data is not co-mingled with the state's data in a virtualized environment. Virtualization provides the ultimate security against compromised computing devices, including mobile phones, since neither data nor applications are stored on the device and can only be accessed from that device by an authenticated user.

Technology alone cannot prevent security breaches. Good information security requires constant training about best practices and emerging threats. Tactics used by hackers to steal data are constantly evolving, and state employees must remain vigilant.

In developing a comprehensive end-user strategy, the State CIO's staff will investigate the cost and benefits of acquiring the mentioned technologies to centrally manage all devises used by state employees to conduct state business. A proof-of-concept program at ITS will be explored to identify additional issues with a statewide end-user strategy.

Roadmap

The short-term goal of establishing an interim BYOD policy is addressed in this report. Over the long term, the State CIO will develop a broader plan and policies for BYOD across state government, expanding the security and compliance approach. Results [PT1]will be[drl2] presented to the Joint Legislative Committee on Information Technology Oversight, pursuant to the BYOD provision in the budget bill adopted in 2013. With approval from the committee, the State CIO will begin implementing the plan.

Issues & Cost

A combination of technology solutions will be required to protect state data and provide secure access to state applications as employees continue to demand access to applications and data around the clock, regardless if the device is owned by the state or the employee. Applications that users need to get their jobs done have expanded beyond just mobile email to include Windows, datacenter, web, and native mobile operating system applications. However, allowing users to access all of their apps and data from untrusted devices raises significant security and compliance concerns, as was mentioned with PII and confidential information.

An integrated approach that secures and manages mobile devices, applications, and data from one centralized point that sets application and data access policies based on device ownership, status, or location is required. Users need secure access to email, applications, data, documents, and the ability to segment their environments into business and personal uses. Depending on a user's persona, the different user types within a targeted population that share similar technology behaviors, a device that is centrally managed via a mobile device management (MDM) solution, managed by providing secure access to their applications through virtualization, or a combination of these technologies is required to ensure employee productivity, security of the state's data, and the segmentation of the user's

personal and business information on the device. Though these technologies provide the necessary security, they are costly in terms of pricing and resources required to implement in the state's environment.

Next Steps

The State CIO is currently testing application and virtual desktop virtualization solutions as an Innovation Center proof-of-concept project across multiple agencies. As was mentioned, these technologies provide modern solutions to securing the state's application and data by providing secure access to a user's desktop or application, completely segmenting the state's data from the user's personal data, regardless of the device used.

When the proof-of-concept effort is completed, a determination will be made if this is a viable solution for the state going forward. In addition to virtualization technologies, the State CIO will explore a multi-agency Innovation Center proof-of-concept project with a mobile device management (MDM) solution to understand the capabilities, interactions with a virtualized user environment, and cost impacts of these types of solutions and to determine the requirements for a procurement as well as any potential change management impacts.

Appendix

Here is the full text of the legislation

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.