Mobile Computing Policy Best Practices

March 2012

1) Assemble the Right Team

Addressing privacy and security concerns properly requires input from many departments across a company. To assemble the right team – one that can ensure that company and employee concerns are best met – include representatives from IT, HR, legal, and relevant business units (e.g., marketing/sales).

2) Identify the Use(s) of Mobile Computing by Employees

A company may permit employees to use multiple types of mobile devices or remote access to efficiently and effectively perform their job responsibilities. These mobile or remote connections may increase employee productivity and provide enhanced convenience, but also may create additional risks to the security and integrity of the company’s network and data. To create a policy that addresses these devices and solutions while minimizing risks, start by taking an inventory of the current and proposed mobile devices or remote access solutions used by company employees.

   a) Remote Access to Company’s Network. Does the company permit employees to remotely connect to the company’s network? What types of devices may connect to the network? Does this include both company-owned computers or employee-owned computers? Is remote access provided through a VPN or similar technology solution?

   b) Mobile Devices. Does the company permit employees to use mobile devices to access company information (e.g., smart-phone, tablet)? Are these company-owned devices or employee-owned devices? Has the company evaluated and addressed potential privacy and security issues? Is all email traffic, including attached documents, pushed to mobile devices?

   c) Mobile Drives. Does the company permit employees to use mobile drives (e.g., portable hard drives, flash or thumb drives)? Does the company require any specific security protections for the use of mobile drives or limit the types of information that may be stored on them?

3) Tailor the Scope of the Policy

Tailor the policy to the specific needs of the company. A policy that meets the needs of one company may be over-inclusive or under-inclusive when applied to another company. A company should consider not only the types of devices used by employees to access the company network or data, but also the types of data that may be accessed on the network or sent to the mobile device.

4) Approval of Devices and Software

If “bring your own device” (BYOD) is accepted, consider whether minimum hardware, software, or security settings should be required before such devices are able to access the company’s network and data. Specific considerations for personal devices include:

   a) Hardware. Are there minimum hardware requirements to connect to the company’s network? For example, must an employee’s personal laptop meet certain hardware performance requirements in order to use the VPN solution provided by the company?
b) **Software.** Are there minimum software or operating system requirements to connect to the company’s network? This may be especially important when a company provided technology solution must be used in conjunction with an employee’s personal computer or mobile device. For example, will the company’s VPN solution work with older versions of a certain operating system? Is the specific operating system on a mobile device supported by the company’s network and IT team? Does the relevant software satisfy the security requirements necessary to protect the data available on the network?

5) **Remote Wipe**

Determine whether the company needs the ability to remotely wipe company content from a mobile device. If so, examine whether this limits the types of devices that may be approved for use or access to the company’s system.

If a remote wipe functionality is used, be sure to obtain the employee’s consent, as it could cause the loss of personal information also stored on the device.

6) **Proprietary and Confidential Information**

Consider how proprietary and confidential information will be handled on the remote or mobile device. This may include employee or customer information that is subject to various federal and state privacy and data security obligations. For example, applicable laws and regulations may require the company to provide reasonable and appropriate administrative, technical, and physical safeguards to protect such employee or customer information. Additionally, even when the company does not have a legal obligation to protect certain information, the disclosure of certain proprietary information may cause a company to lose other legal protections. For example, disclosure of certain information may result in loss of trade secret or confidential protection of such information or harm a company’s competitive advantage. Consider restricting the ability to store such data locally, or only permitting local storage when data is encrypted.

7) **Technical Security**

Ensure that technical safeguards for mobile devices or remote connections are consistent with the company’s information security policies, and relevant laws and regulations, including provisions for user IDs, passwords, and other authentication methods, as well as antivirus or malware programs, and security patches. For example, the Massachusetts regulatory standards for the protection of personal information prohibit the transmission of unencrypted personal information over public networks or wireless networks.

8) **Retention and Disposal**

Identify whether remote access and mobile device users are permitted to create hard copy documents (print outs) or locally-saved copies of company documents or data, and establish how these items must be protected or destroyed during and after use. Consider whether these items may only be retained for a certain period of time. Additionally, ensure that the policy requires such items to be disposed of in a manner compliant with the company’s document retention and disposal policy, as well as relevant federal and state laws governing the disposal of personal information.
9) Review and Revise the Policy on an Ongoing Basis

A policy that fits the structure and needs of the company today may not meet the company’s needs in the future—especially with the rate of change in current technology offerings. A company should regularly review its mobile computing policy to ensure that it reflects the technology solutions used by the company and the current and foreseeable risks to the company’s network and data.

Contact

John J. Heitmann
jheitmann@kelleydrye.com
(202) 342-8544