SMITH ANDERSON
expectexcellence®

BRING YOUR OWN DEVICE WORKPLACES - PROGRAM CHECKLIST

01.09.2014
Kimberly J. Korando

Identify the BYOD Program Planning Team (e.g., IT, HR, Legal, others?)

Identify Threshold Scope Issues. For example:

1. What data/information will be accessible on BYOD devices?
    - Does the organization have trade secrets or other proprietary or highly confidential information that require special protection measures to qualify for protection under trade secret and related laws? Trade secrets laws typically require that the organization prove that it took “reasonable measures” to protect the information; and
    - Does the organization have data/information that is regulated by federal/state privacy laws (e.g., financial information, health information, personal identity information)?
2. Will BYOD be available to all employees or are some excluded (e.g., senior executives, R&D, sales, non-exempt, contingent, international workers, unionized workers)?
    - Will different approaches be taken with employees who have access to highly confidential or other protected information?
    - Is there a collective bargaining agreement that covers included employees? If so, BYOD for these employees may be a mandatory bargaining topic.
3. Will there be limitations on the types of permissible BYOD devices?
    - Factors to consider include security issues with particular devices, IT ability to support or collect data from particular devices/operating systems.
4. Will BYOD be mandatory or a privilege?
    - Employees are more compliant with BYOD programs that are a privilege as opposed to those that are mandatory.
5. Will organization provide help desk support for BYOD devices? If not, what security precautions will need to be taken to protect company information from third party vendors?

Determine the Appropriate Technical Controls. For example:

1. Mobile Device Management (MDM) software:

- Gives organization some control, but does not totally resolve issues; and
- Selected MDM may limit devices and operating systems that can be used.

2. Sandbox company information (versus allowing syncing and commingling of personal and company data);
3. Allow access to, but prohibit download of, certain information;
4. Encryption of data;
5. Passwords;
6. Device tracking;
7. Remote wiping; and
8. Block installation of prohibited apps.

Determine the Appropriate Policies and Procedures:

1. Policy decisions will be based on a number of factors, including the type of employees, the type of data and degree of confidentiality, company's acceptance of risk; and
2. Decide whether a separate stand alone policy will be issued or existing policies revised to address BYOD.
    - Stand alone policy should properly cross-reference other related policies.
3. Examples of policy provisions to consider:
    - Require that employees obtain IT authorization for each personal device/require IT to maintain inventory of each personal device;
    - Require that employees adhere to a "required/prohibited" app list;
    - Specify prohibited/acceptable devices;
    - Prohibit jailbreaking/modding devices;
    - Prohibit shared use of devices (unless company information is sandboxed;
    - Require compliance with all security procedures (e.g., encryption, passwords, anti-virus software, no upgrades unless company approved, no syncing or unauthorized back-up or storage, no disabling security or other systems);
    - Prohibit use of "clouds" (e.g., Dropbox, Evernote):
        - Under Federal Stored Communications Act, the company may not be able to get its data back from employee's "cloud" account; and
        - This issue also applies to company-owned devices.
    - Require immediate notification of lost or stolen device:
        - After certain time ability to wipe data remotely may be lost.
    - Non-exempt employees must report all "off-duty" time spent on company business using personal device;

- All other policies apply when personal device used on work time or premises; and
- Identify and revise other applicable policies, as needed (e.g., harassment, data privacy/ security, time worked/reporting, confidentiality, record retention, computer use).

Determine Privacy and Company Access and Control Issues:

1. What expectation of privacy will employees have to data (company and personal) on personal device?
2. Will activities that are prohibited on company devices (e.g., viewing pornography) be prohibited on personal devices?
3. What monitoring will be done (e.g., when connected to company network, data transmission, on device)? Just sandbox or entire device?
4. How will the company protect against employees /consultants bringing another party's (e.g., former employer) information into the "workplace"?
    - Require employee/consultant representation that s/he has properly cleared BYOD device of information from prior jobs and agrees to no improper use of another's information.

Require User Agreement

1. Policies without User Agreement are insufficient to protect the company because policies are not contractually binding on individual. Moreover, authority to use personal device should serve as consideration for agreement;
2. Recommended provisions include:
    - Policy Compliance (spell out key requirements, prohibitions listed above);
    - Notification requirements n case of lost or stolen device, including timing and to whom.
    - Consent to company to install security software, monitor device, access (including provision of login credential), copy, wipe/brick, exit interview/inspection and wipe/ certification of compliance, device forfeiture on demand (access, copy, wipe also apply to personal information, especially in the event of litigation hold responsibilities or investigations):
        - If company information is not sandboxed and company does not have employee consent to wipe data, then company may be liable for destruction of employee's personal information that is wiped
    - Requirement that company data be retained until company can copy data, including back-up;
    - Device disposal requirements;
    - Acknowledgement that company owns company information on personal device; and
    - Acknowledgement that company is not responsible for loss, damage, loss of use, liability.

Internal Investigations/Record Preservation/eDiscovery

1. Does IT have the expertise to collect data/copy data on the personal device/operating system?

2. Ensure that litigation hold notices include personal devices; and
3. Ensure that policy and user agreement includes requirement that device be forfeited to company and all data (including personal data) copied in these events.

Identify Expense Reimbursement/Tax Issues/Cost of Repair

PRESENTATION MATERIALS (PDF)

PROFESSIONALS

Kimberly J. Korando

PRACTICE AREAS

Data Privacy

Non-Compete & Trade Secrets