MILLER CANFIELD

Don’t Let BYOD Become LFYO (Liability For Your Organization)

June 11, 2012

"BYOD" stands for "bring your own device," the practice of allowing employees and contractors to use personal devices, such as laptops, smartphones, home computers and tablets, to conduct the organization's business. The lack of control over company information accessed and stored on personal devices can lead to legal issues involving privacy, security and data retrieval. Whose responsibility is it to protect and secure a BYOD smartphone? What happens to company data if the personal tablet is lost or stolen? What privacy rights does an employee have with respect to personal data stored on a BYOD notebook? Can an organization be sanctioned if a contractor deletes company data from a personal laptop that falls within the scope of a litigation discovery request? What happens when an employee using a BYOD device leaves the organization?

These and other questions should be considered by any organization allowing BYOD. A thoughtfully drafted BYOD policy will address ownership and control of business data, privacy expectations for personal data, security requirements, procedures for lost and stolen devices, exit procedures and consequences for violations of the policy.

Is a "NO BYOD" policy the answer? Perhaps, but consider that, according to Juniper Network's Trusted Mobility Index survey from May 2012, 41% of the over 4,000 mobile device users surveyed admitted to using their personal device for business purposes without company support.

Whether your organization allows BYOD or not, a workable policy to address the myriad of legal issues raised is a must. The full Juniper survey is available here.