June 2013 HR White Paper

Bring your own device (BYOD) policy Q&A

Has your company recently implemented a bring-your-own-device (BYOD) policy for electronics? In short, a BYOD policy is one in which the employer allows the employees to use their own personal devices for work use rather than requiring separate work devices to be used. Implementing such a policy can be a complex issue as employers must balance employee privacy needs with legal compliance issues all while ensuring that everyone is on the same page in terms of how the policy will function.

More companies are adopting BYOD policies and more employees are starting to expect it – particularly younger employees who want to use their own devices.

This is something that will continue to be on the radar. Even if your company is not thinking of this now, it may come up in the near future as the culture changes.

In a recent BLR webinar, Jason Storipan gave some guidance on this new trend. He answered participant questions about drawing the line between work and personal use and to be aware of the biggest implementation obstacles. Here are some of the employer questions from the webinar and Storipan's answers.

Q. How do you draw the line between personal and work use (especially as it relates to visiting sites that would be inappropriate on a work device)? This is a personal device, but used for work. Can you discipline for visiting inappropriate sites if the employee says it was visited on personal time?

A. Employers need to set expectations that the devices will be monitored, and employers also need to establish what will and will not be tolerated in terms of internet use. Then the employees will have the option to use other devices for things that would be deemed inappropriate for work devices. The key is to set the expectations clearly, including the disciplinary actions that will be taken.

Q. Is there a standardized BYOD policy that can be used to govern employee use of personal devices for work?

A. This comes down to each employer's needs. A general, one-size-fits-all policy is not recommended since it may not address your company's needs. You need to be sure you talk with everyone involved, including an attorney, to ensure the company's needs are met.

Q. If a company decides not to adopt a BYOD policy, are there legal implications?

A. If you chose to not allow the employees to access the network from their personal devices at all, there are no legal implications in that regard. There's not a "right" to access the network at home, for example. If the company provides a phone instead of having employees use their own, that is also perfectly fine. In fact, it's perfectly fine to disallow access offsite.

However, where you get into trouble is when you let employees access the network through personal devices without having any policy or set expectations. Employers need to ensure employees know what level of privacy can be expected (or not expected) when accessing the network, what actions can be disciplined, etc. Even if you're not allowing access outside the workplace, that should be outlined.

Q. What's the most difficult obstacle in implementing a BYOD policy?

A. Getting everyone on board is probably the most difficult. Getting agreement – especially since there will be additional work for some people – is often a catch. For example, the IT team must often monitor additional devices and varied devices. Making sure the software is compliant for all types of devices can be another area where extra work is involved.

Involving lawyers in the process is also a question – any adverse situation will now add a whole new level of complexity with the need for e-discovery across personal devices (and it's more difficult to monitor them). Typically, high-level executives are behind the idea because they like to use their own devices, but sometimes they may be reticent when it comes to concerns about data security or privacy