BRING YOUR OWN DEVICE:
DEVELOPING AN EFFECTIVE BYOD POLICY FOR YOUR BUSINESS

Since the practice emerged close to a decade ago, an increasing number of employees have been using their own laptops, tablets and smartphones for work-related tasks, both on- and off-site. Today, many tech- savvy companies – including Intel, IBM, Workspot and Cisco – not only condone the practice, but actively encourage it.

What they and thousands of other large and small employers have discovered is that Bring Your Own Device programs (BYOD) can boost efficiency and productivity and enhance employee satisfaction, as many employees are more comfortable with their own devices than with those provided by their companies. In addition, by shifting the burden of technology acquisition to employees – many of whom are apt to voluntarily update their devices on a regular basis – employers can save a significant amount of money.

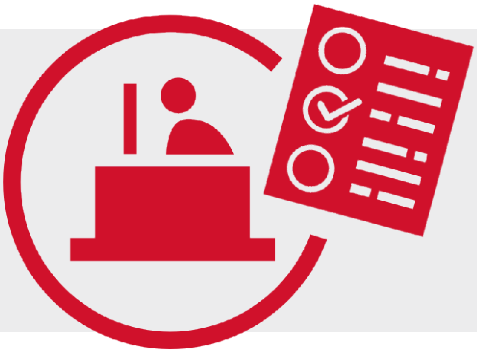
In short, it's all good. Well, almost. Because while BYOD is proven to boost employee morale, increase productivity and cut costs, like BYOB, it needs to be implemented with care, lest things get out of control. So, before you move forward with a BYOD program, it is important that you develop a formal BYOD Policy covering issues such as network access, security, confidentiality, reimbursement and more.

Getting Started: The Basics for Every BYOD Policy

While your final BYOD Policy will be "customized" to reflect your company's technology use, staffing, network infrastructure and internal culture, there are certain essential considerations and issues that must be addressed by every employer, regardless of company size or type.

First, you must set basic parameters regarding connections to your company's network, systems and database. Ask yourself overarching questions such as:

- Will you allow unlimited access with personal devices?
- Will you limit access to non-sensitive systems and data?
- Will you insist on IT control over personal devices, applications and stored data?
- Will you prohibit storage of company data on personal devices?



Once you've answered these questions and established the basic foundation for your BYOD Policy, you can drill down to develop specific rules and guidelines in key areas including:

Devices

Your policy must include explicit rules on which devices can be used for work-related tasks. Your IT manager will determine which devices pose unacceptable security risks and/or are not fully or easily compatible with your network, systems or database. Device prohibitions will differ from company to company.

Acceptable Use

Your Acceptable Use policy defines how a personal device may be used during business hours. It may also cover what personal uses are prohibited after business hours because they pose a threat to data or device integrity.

Security Procedures

Security policy covers a number of key issues, including prohibited downloads and specific procedures to be followed if a device is lost, an employee leaves the company, or a breach is detected. The most important step will be to establish iron-clad password protocols. At a minimum, you should require two-factor authentication and regular updating of passwords.

Support Services

Your policy should include specific direction on how to address technical support issues. It is important to clearly state the circumstances under which an employee is required to consult IT, and what rights IT has in terms of monitoring and modifying devices belonging to the employee.

Reimbursement

While the bulk of the cost for technology acquisition will be borne by the employee, your BYOD policy must include guidelines on reimbursement rates for phone and data plans, data overages, device upgrades and replacements.

Clearly, these are just basic guidelines for the development and implementation of a complete and fully-effective BYOD Policy. Your IT manager or a professional IT consultant will be able to provide more details and specifics. In addition, there is a wealth of information available online. Regardless of how you choose to proceed, it is essential that your BYOD Policy is in place before you integrate personal devices into your company's technology mix.

LONG ISLAND TEMPS

516 631 777-TEMPS (8367)
www.LongIslandTemps.com