Look at the benefits of BYOD (Bring Your Own Device) and it is easy to see why both workers and employers often support the arrangement. Employees can select the tech with which they feel most comfortable and enjoy access to both work-related and individual information in one convenient place. To a company’s advantage, BYOD spares (or at least lowers, if sharing costs) the business expense of issuing smartphones, laptops, or tablets. And staff members possessing the means to connect from any place at any time raises productivity potential, especially while traveling or when an emergency closes the office.

The set-up, however, also contains a variety of potential pitfalls that both sides need awareness of from day one. Here, we examine some of the risks of BYOD and actions to combat these dangers.

**Risks of Bring Your Own Device**

Using tech always involves some risk, which is why companies perform safety measures such as installing anti-virus software and requiring passwords to access files. IT departments keep in-house machines up-to-date on security and permissions, and computers never leaving the office minimizes chances of being lost or stolen.

Much of that control gets compromised when devices are not company-owned and routinely move outside the office. Owners may not diligently keep up on security patches. Outsiders may view the files an employee has open or hack into them. Devices can be forgotten anywhere.

Keeping company interests top-of-mind also can be problematic. When an employee owns a device, he may not operate as carefully on it as compared to a machine clearly marked solely for work. He may decide to delete business messages that should have been saved, leading to potential problems if the content is ever needed for legal cases. The employee also may not realize that inappropriate cyber behavior, such as sending sexually explicit photos to a colleague, isn’t “excused” because executed on his own device -- landing both the worker and the company in a great deal of hot water.

Malicious behavior on the device becomes an immediate issue if an employee gets terminated. Without swift action to prohibit access to files and permanently wipe off company information, an angry former employee may tamper with records and other proprietary or confidential data.

**Creating electronic policies and procedures**

Protecting the company starts with clear, written instructions governing the use of personal devices. Because of the importance of such a document and all the aspects to consider, input needs to come from a variety of relevant sources, including legal counsel, senior executives, HR, records managers, and IT.

While companies formulate BYOD policies and procedures based on their own needs, the following are often at the heart of what should be covered:
• User will password-protect the device in accordance with company standards.
• User agrees to maintain the original device operating system, keep the device current with the manufacturer’s security updates and patches, and allow company IT to install security (firewall, antivirus, web protector applications) as seen fit.
• User will not install software to bypass standard built-in security features and controls.
• User agrees the device will not be shared with family, friends, or other individuals.
• User will follow company rules governing what employees may and may not do with business records & HR information on personal devices. This includes agreement to delete sensitive business files that may inadvertently be downloaded/stored via email attachments. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a complaint or lawsuit, proprietary information, company financials, and other business records.
• User will forward business-record text messages, email, and other electronically stored information to business email accounts at the end of each workday.
• User must notify management immediately if device is lost or stolen.

Guidelines also often require employees to let IT examine personal mobile devices as necessary. As this can be a controversial action, take care to craft a sensitive statement, such as this sample:

The company will respect the privacy of your personal device. We will only request access to your personal device by company IT to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if the user downloads business records, email, attachments, or other company documents to a personal device).

Note that this differs from a company’s policy for employer-provided mobile devices and services. Employees do not have the right, nor should they have the expectation, of privacy when using company-owned mobile devices or services.

**What about when an employee leaves?**

A BYOD policy also should address what happens when an employee leaves the company. Workers need to know that IT will wipe (delete) business data and HR records stored on the device at the time of departure. Consider developing a protocol to protect employees’ personal, insignificant information -- while removing all business records, HR information, other company data.

Remember, though, that guidelines mean little if just tucked away. For them to be effective, give employees a clear understanding of their individual and collective roles when it comes to lawful record management and compliant online behavior. Educate workers not only about what policies exist, but also how these words apply to everyday actions. An educated staff serves as a great first line of defense by preventing problems before they start!