For many employees, the line between work and personal life has grown increasingly murky. Many now use their own tech gadgets to do business as often as they use company property. On the one hand, that can save the company money on hardware and make employees more efficient. But it also presents serious security risks. Short of banning employees from accessing work files with personal equipment altogether, there are five things businesses must keep in mind when it comes to employees using their own mobile device in the workplace.

1. Have a Policy & Communicate It
Take control of managing the retention of documents, especially business-critical information. To ensure a strong, manageable approach to data retention, companies need to create and distribute a policy that outlines what is and is not acceptable for employees to do when it comes to personal mobile devices, applications and other tech tools. Companies should also organize periodic training sessions that cover issues such as social media usage, protecting personally identifiable information, creating strong passwords and maintaining proper privacy settings so that employees can clearly understand the appropriate and inappropriate uses of their personal devices.

2. Know Regulatory Requirements
When you are utilizing an organization's device, regulatory requirements for storing documents typically apply. This concept must also be applied to people using personal devices to do company work. Companies need to work with employees to ensure that all devices, both personal and professional, meet regulatory standards.

3. Back Up Often
Users who opt to use a personal device at work need to understand that their employer is not responsible for managing and protecting their personal data. Most consumers don't run out and buy a backup system for their personal devices, but they should be aware of the many options available to them and proactively look for a backup scenario that works for their lifestyle. For example, an easy and effective way to back up data is through an online system. This gives users faster recovery if an issue does occur and provides multiple access points to data so employees don't have to carry around physical storage such as a USB stick or external hard drive. Organizations should consider creating official backup/archiving repositories that mobile devices can access, such as cloud-based storage solutions, rather than leave individuals to find their own solutions.

4. Be Aware of Your "Personas"
For most, organizing your data and respective communication accounts to support different "personas" isn't an issue. However, business professionals should always try to keep their business and personal life separate. The advent of social media has made this more difficult, as many people now have one account where they showcase who they are in both lives. As these personas blend into one, users often make comments or post status updates before thinking about who they represent as an employee.

5. Know Who Owns What
With the evolution of personal devices, it is very easy for users to have access to multiple personas at their fingertips both in and out of the workplace. Users should be advised that any work done on a personal device related to business belongs to the business and not the user. If the employee should lose the device or it should fall into the wrong hands, the user's workplace can reserve the right to wipe the data remotely. Organizations need to make employees aware of the policies for the authorized work-storage environment from the beginning.

Wayne Wong is managing consultant at Kroll Ontrack