Mobile Device Remote Scrub Waiver

Remote wipe technology is a self-destruct button enabling you to keep lost, stolen or otherwise compromised smart phones, laptops, tablets and other mobile devices containing precious confidential data from falling into the wrong hands. However, pushing the button can become problematic when the data you want to wipe is contained on a device personally owned by an employee. That's why it's essential to establish your right to wipe remotely as part of the deal you make in return for allowing employees to connect their devices to your network. Here's a template of a waiver agreement that you can adapt for your own circumstances.

1. POLICY

ABC Company uses remote wipe technology to erase data contained on lost, stolen or otherwise potentially compromised mobile devices to ensure the integrity of confidential Company business and customer data the mobile device might contain or enable access to. All users of mobile devices that connect to an ABC Company network, and/or are capable of backing up, storing, or otherwise accessing data of any type, must agree to this remote wipe waiver.

2. POLICY

The purpose of this Waiver is to ensure that the undersigned employee understands how and why ABC Company uses remote wipe technology and secure his/her knowing and voluntary agreement to use of that technology to wipe data from his/her own mobile device in the event that it becomes necessary. This waiver is to be read with, and signed in conjunction with the ABC Company Mobile Device Acceptable Use Policy ("Policy").

3. SCOPE OF POLICY

This Waiver applies to the same devices and users outlined in the Policy to the extent such devices are used to access ABC Company resources in accordance with the Policy.

4. REMOTE WIPE

Employee understands that in connecting to ABC Company technology resources, mobile devices come under the ABC Company's IT department's authority and capability of being wiped remotely in the event the device is lost, stolen, or compromised in any way. Remote data wiping is essential to protect the Company and its clients. When and

if IT or an employee/user initiates a remote wipe, the user’s mobile device will be wiped of all data, documents, files, settings and applications

Employees/Users may also request a remote wipe of all data stored on that device. They can later restore personal date from a personal computer or a cloud service. It is recommended that employees backup their personal data frequently to minimize loss if a remote wipe is necessary.

A remote wipe will only be initiated if IT deems it appropriate. Examples of situations include, but are not limited to where…