TRUCE®

A Guide to Creating an Effective Mobile Device Policy

Businesses today rely on employee's ability to access mobile business applications from their mobile devices. In fact, 79% of executives view mobile phones as necessary for employees to do their jobs effectively.[1] So why is it that less than half of decision-makers believe their current mobile device policies meet current safety or productivity needs?[2] A strong policy is the start to keeping mobile devices useful and secure while also protecting the safety of the employees.

Tips on Creating and Implementing Your Policy

Consult with other stakeholders.

All employees are impacted by how and when mobile devices are used in the workplace. An effective policy addresses the needs of the entire organization, from executives, to managers, to frontline workers. By working with the various stakeholders across your organization to understand how and when a mobile device is required, and what guidelines they'd like to see established, you can create a more robust policy that accommodates how people actually work at your organization. Involving employees in the process provides the added benefit of compliance once the policy is rolled out.

View your policy as a way to reinforce your business strategy.

Why does your company rely on mobile devices to get work done? How and when should your employees be using them? What circumstances or environments require tighter or looser device management? Be as specific as possible in the policy so that everyone reading it understands how the right use of mobile devices impacts the business and the individuals in meeting their goals.

Elements of an Effective Mobile Device Policy

Company policies can vary when it comes to length and complexity – everything from high-level do's and don'ts to page after page of detailed discussion around acceptable use. Whatever the style for your company, the following components of an effective policy should be incorporated into the final document:

1. Scope

Determine what constitutes a mobile device as it relates to the policy. Most organizations will choose either Company-Provided or Bring-Your-Own-Device (BYOD) programs, or a combination of the two, to enable the mobile productivity of their workforce. Will the policy cover just corporate-issued devices and bring-your-own-devices, or does it also cover personal phones brought on site for personal use? Establish this right up front so everyone understands what's in and what's out.

2. Business Requirements

How are mobile devices used at the workplace? Why are they critical to business operations? Are there specific roles that have a higher need for mobile access? Use this section to clarify the business strategy behind the use of mobile devices at your organization.

Define the steps needed to secure both the device and your network.

Ensuring safe and secure access to your network and proprietary data is the responsibility of both the company and the employee. Make sure your policy defines both the employee and company obligations. Specify what those obligations are: i.e., the complexity of passwords, requiring employees to deploy device management software on personal devices, or detailing a checklist of security upgrades an employee-owned device needs to pass before it can be used for work.

Find the right person to write the policy.

Whether the policy is drafted by IT, HR, EHS, or Operations, it should be written in clear, easy to understand language to ensure the highest compliance.

Be consistent in the implementation of the policy.

No policy is worth implementing if individual employees are able to use different standards to dictate their work habits, or worse, can choose whether or not to follow the rules. Define how the policy will be rolled out and how you will audit compliance over time.

Educate your employees and keep awareness high.

When done right, the policy is not viewed as something "done to the employee" but as a platform for everyone to support in order to protect what's most important – employee safety and the integrity of the company's network and proprietary data. Make sure employees are educated on not just the terms of the policy but the "why's" behind it. Offer insights on industry and your own organization's safety trends, cybersecurity trends and productivity trends.

Sources

1. How Companies Go Mobile (slideshow). Oxford Economics and Samsung. 2018 study with a follow up study in 2022.
2. Unleash the Full Potential of Mobile with Contextual Mobile Device Management, a Forrester Consulting Thought Leadership Paper commissioned by TRUCE Software, August 2019.

Get software to automatically enforce your policy at **trucesoftware.com**.

TRUCE®

3. Employee Obligations

Make sure your policy details what is considered appropriate use and be specific about the use of apps and features in different situations. What may be appropriate use in a break room is probably not acceptable on a production floor. Be sure to also include the employee's responsibility when it comes to the security of the device. What are your requirements for passwords? Is there a security checklist they need to follow if they want to bring their own device on site and access company networks? It's common in any policy for there to be a user requirement to install security software on the personal device. Establishing the right guidelines can make it easier for employees to understand and thus comply with the policy. Communicate what disciplinary action will be taken for non-compliance.

4. Company Obligations

Following the employee obligations, it's important to show the other side of the equation, namely what your company will be doing to support the policy. If you have a BYOD program, state what the approval process (if any) looks like along with any reimbursement commitments. What tools are you implementing, such as endpoint management software or Contextual Mobility Management (CMM) platforms, to ensure the safe and secure use of mobile devices during work?

5. Signature

Make sure your employees acknowledge not only that they have read and understood the policy, but that they agree to the terms set by that policy. With the company representative's signature, you're acknowledging the importance mobile devices have in the workplace.