



An End to Lost Business Smartphone Worries

With these **21 tips**, organizations can ensure the highest level of data protection when a device is lost.



What is inconvenient with lost private smartphones can quickly become a serious security problem with corporate devices.

Any unauthorized person who gets hold of the device can under certain circumstances access corporate data. This should be prevented at all costs.

The Foundation for Data Protection: A Mobile Device Management System

One of the essential preconditions for averting data loss, in other words, the most **important tip** of all, is the use of a mobile device management system (MDM). **Only with an MDM system can policies be centrally defined and enforced in terms of the highest data security, which then ensures targeted protection of your data.**

1. Specify and Enforce Password Requirements

The IT department can specify in the administration portal which requirements the password must meet to unlock the smartphone or tablet. If the employee does not complete these requirements, they cannot use the device. A secure password consists of at least eight characters and uses all available characters, such as upper and lowercase letters, digits, as well as special characters.

2. Activate Screen Lock on Mobile Devices

If a device is lost, you should first try to locate and retrieve it. If this is not possible, you can select the device in the administration portal and lock the screen. It makes sense to display the lock screen with your organization's contact information so that honest finders can contact you.

3. Lock Workspace on Android devices

In case of loss, the entire workspace on an Android device can initially be locked in the administration portal.

4. Completely Reset Mobile Devices or Remove Workspace

If the device cannot be found again without private usage permission and has definitely been lost, it can be reset to factory settings via the administration portal. Of course, this is not possible for private devices. In the case of BYOD devices, i.e. private devices that are also used for work purposes, the business area on the device can be deleted separately.

5. Hide Notification Content on the Lock Screen

Via notifications on the lock screen, third parties can extract information about the owner of the smartphone (example: incoming emails, chat messages). Such notifications should therefore be prohibited.

6. Reset Mobile Device Passcode

It may be useful to reset a device's passcode via the administration portal so that the device is useless to outsiders.

7. Enable Lost Mode for Mobile Devices

Enabling lost mode allows devices to be located in the console even if location services on the device itself are turned off. The device only needs to be turned on for this to work. Again, this does not work for private devices.

8. Two-Factor Authentication

For additional security, use two-factor authentication of the Google or Apple account that is set up on the device.

9. Use Apple Device Enrollment AED (formerly DEP) and Zero Touch

If you use AED and Zero Touch, make sure the devices can only be used for work purposes with their MDM and are unusable by third parties even after a factory reset.

10. Perform Regular Security and Operating System Updates.

If possible, enforce automatic OS updates to also get regular security updates for the device.

11.Enable the “Find My Device” Feature in System Preferences

For both Apple and Android devices, you can enable a service to find your device. Here is a guide on how to [find an iPhone](#) and [a guide on what to do to locate an Android device](#).

12. Define/Enable Automatic Screen Lock Time

Enable an automatic screen lock. For example, you can set the smartphone to lock when it has not been used for a certain amount of time. However, do not choose too short a time, otherwise, it will hinder productivity.

13. Set Maximum Number of Failed Login Attempts

Set a maximum number of failed attempts to unlock the device and block its use by unauthorized persons.

14. Enable Factory Reset Protection (FRP) (Android) and Activation Lock (Apple)

Even if a third party can reset the device to factory settings, a device protected with FRP cannot then be set up with a private Google account. The use of Android Zero Touch and DEP for Apple devices also helps. Apple uses the Activation Lock in the same way. This works in the same way and is automatically enabled by activating “Find my device”.

Further Tips for Securing Your Devices and Data

15. Use Android Devices Recommended by Google

If you decide to use Android smartphones or tablets, be sure to choose devices that are on the [list of devices recommended for corporate use](#). These have been vetted by Google and are suitable to be managed with an MDM system.

16. Inform Employees

Make it clear to employees that an enterprise remote wipe will not delete their personal data. That way, you can be sure that a lost device will be reported to you more quickly.

17. Implement a BYOD Program If Applicable

With a BYOD program, employees use their own personal devices for work and are compensated a share of the device costs or fees. An advantage in terms of security is that with private cell phones, employees notice the loss quickly, and report it to you without delay.

18. Obtain Appropriate Insurance

Be sure to obtain suitable insurance for your devices.

19. Use of Cloud Services/Cloud Storage

If your employees use cloud services, the data stored in the cloud is also secured in the event of device loss.

20. Conclude a Formal Agreement with Employees

When employees are provided with company devices, they should sign a formal agreement that outlines how the devices should be handled in terms of security. Such a document not only safeguards the company but also raises employees' awareness of security issues. For example, it must be clear to employees that they must report any loss of equipment immediately.

21. Use Protective Accessories

To protect the device against damage, you should use protective screen covers and suitable cases. If you buy or rent corporate devices from Cortado, we will also make recommendations for suitable accessories.

Do you have any questions about securing or even managing your organization's devices? Then we look forward to hearing from you at sales@cortado.com.

Do you want to trial Cortado MDM free of charge and without any obligation? Then please use our [demo link](#).

