3.8.2 Mobile Device Security Facts

Mobile devices include smart phones, laptops, tablet PCs, PDAs, and other small handheld computing devices. These types of devices require a subset of security considerations when stolen, misplaced, or lost.

Consideration	Description
Request Process	Mobile devices will usually contain confidential information, thereby creating a security risk for an organization. To control the risk, an organization should control who is issued a device and what information is put on the device.
Asset Tracking and Inventory Control	Because mobile devices are not tied to a physical location, asset tracking and inventory control are very important. At a minimum, you should track the following for each device owned by your organization: ▪ The make and model number of the device ▪ The device serial number ▪ The operating system version number ▪ The date the device was purchased and the vendor it was purchased from ▪ The end-of-warranty date for the device ▪ The vendor providing support for the device ▪ The employee to whom the device has been issued There are many mobile endpoint management solutions that can be implemented to automate asset tracking and inventory control processes. Most of these solutions can also use the following technologies to track the physical location of your mobile devices: ▪ The Global Position System (GPS) can track the location of GPS-enabled devices to within a meter. ▪ Wi-Fi triangulation can track the location of devices in heavily-populated urban areas to within a few meters, depending upon the number of networks in range and the accuracy of their signal strength data. ▪ Cell phone tower triangulation can track the location of devices to within a kilometer, depending upon the signal strength and number of cell towers within range. ▪ IP address resolution is much less accurate than the other options, tracking the location of devices to within roughly 20 kilometers.
Acceptable Use	The acceptable use policy should define personal use and after-hours use. Irresponsible, illegal, or malicious use of the device could leave an organization liable for damages if such use is not prohibited by a policy.
Personal Identification Number (PIN)	All devices should be accessible only after a PIN has been entered or another authentication method has been activated.
Unused Features	Just as with a desktop or server system, you should disable or uninstall unused features on mobile devices. Unused features or services can expose threat vectors into the device.
Lockout or Screen Lock	A lockout (or screen lock) disables the ability to use the device after a short period of inactivity. The correct password or PIN unlocks the device.
Encryption	Data encryption ensures data confidentiality on the device. Voice encryption (on mobile phones) ensures data confidentiality during transit.
Remote Wipe	*Remote wipe*, also known as *sanitization*, remotely clears specific, sensitive data on the mobile device. This task is also useful if you are assigning the device to another user or after multiple incorrect password or PIN entries.
Storage Segmentation	Consider segmenting personal data from organizational data on mobile devices. This storage strategy allows: ▪ Encryption to be applied only to sensitive organizational data on the device. ▪ Only organizational data to be removed during a remote wipe, preserving personal data.
Reporting System	A procedure to immediately report the loss of a device will enable the device to be disabled quickly and reduce the chance of confidential information being compromised.

All employees who use mobile devices should be trained on the security considerations and the reporting process in case the device is stolen.