11.4. Mobile Telephony

Objective

11.4.1. Mobile telephone systems and devices are prevented from communicating unauthorised classified information.

Context

Scope

11.4.2. This section covers information relating to the secure use of mobile telephones, tablets and other mobile, voice communication capable devices, as well as the systems they use to communicate information.

11.4.3. Mobile devices use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, and NFC frequencies. All such mobile devices are considered to be transmitters.

11.4.4. Mobile devices with cellular capability will regularly "poll" for the strongest signal and base or relay station. Monitoring such activity can be used for later interception of transmissions.

11.4.5. Information regarding Voice over Internet Protocol (VoIP) and encryption of data in transit is covered in Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony and Section 17.1 - Cryptographic Fundamentals.

11.4.6. It is important to note that VoIP phones have some of the same vulnerabilities as the mobile devices discussed in this section.

11.4.7. Mobile devices can be equipped with a variety of capabilities including internet connectivity, cameras, speakerphones, recording and remote control. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to mobile devices with 3g/4g/5g capability.

PSR references

11.4.8. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Mobile device usage policy

11.4.9.R.01. **Rationale**

All mobile devices are subject to interception. The required level of expertise needed varies greatly. Accidentally or maliciously revealing classified information over mobile devices can be intercepted leading to a security breach.

11.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2691]

Agencies MUST develop a policy governing the use of mobile devices.

Personnel awareness

11.4.10.R.01.

Rationale

There is a high risk of unintended disclosure of classified information when using mobile devices. It is important that personnel are aware of what levels of classified information they discuss as well as the wide range of security risks associated with the use of mobile devices.

11.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:2694]**

Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external mobile devices.

11.4.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should [CID:2695]**

Agencies SHOULD advise personnel of all known security risks posed by using mobile devices in areas where classified conversations can occur.

Use of mobile devices

11.4.11.R.01. **Rationale**

When classified conversations are to be held using mobile devices the conversation needs to be appropriately protected through the use of encryption measures and a secure network.

11.4.11.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must [CID:2698]**

Agencies intending to use mobile devices for the transmission of classified information MUST ensure that:

- the network has been certified and accredited for the purpose;
- all classified traffic that passes over mobile devices is appropriately encrypted; and
- users are aware of the area, surroundings, potential for overhearing and potential for oversight when using the device.

Mobile Device Physical Security

11.4.12.R.01. **Rationale**

Mobile devices are invariably software controlled and are subject to malware or other means of compromise. No “off-hook” or “power off” security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.36.

11.4.12.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must [CID:2701]**

Mobile devices MUST be prevented from entering secure areas.

11.4.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should [CID:2702]**

Agencies SHOULD provide a storage area or lockers where mobile devices can be stored before personnel enter secure or protected areas.