22.2. Working Outside the Office

Objective

22.2.1. Information on mobile devices is not accessed from public or insecure locations.

Context

Scope

22.2.2. This section covers information on accessing information using agency-owned mobile devices from unsecured locations outside the office and home environments. This section does not apply to working from home; requirements relating to home-based work are outlined in Section 21.3 – Working From Home. Further information on the use of mobile devices can be found in Section 21.1 – Agency Owned Mobile Devices.

22.2.3. Also refer to Chapter 12 - Product Security for requirements on product security, selection, maintenance, sanitisation and disposal.

Rationale & Controls

Working outside the office

22.2.4.R.01. **Rationale**

As the security risk relating to specific targeting of mobile devices capable of processing highly classified information is high, these mobile devices cannot be used outside of facilities certified to an appropriate level to allow for their use. In addition, as agencies have no control over public locations including, but not limited to, such locations as public transport, transit lounges, hotel lobbies, and coffee shops, mobile devices are **not** approved to process classified information as the security risk of classified information being overheard or observed is considered to be too high in such locations.

22.2.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4541]

Agencies MUST NOT allow personnel to access or communicate classified information on mobile devices outside of secure areas unless there is a reduced chance of being overheard and having the screen of the device observed.

22.2.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4542]

Agencies allowing personnel to access or communicate classified information outside of the office SHOULD NOT allow personnel to do so in public locations (e.g. public transport, transit lounges, hotel lobbies and coffee shops).

Carrying mobile devices

22.2.5.R.01. **Rationale**

Mobile devices used outside the office are frequently transferred through areas not certified to process the classified information on the device. Mechanisms need to be put in place to protect the information stored on those devices.

22.2.5.R.02. **Rationale**

When agencies apply encryption to mobile devices to reduce their physical transfer requirements it is only effective when the encryption function of the device is not authenticated. In most cases this will mean the mobile device will be in an unpowered state (i.e. not turned on), however, some devices are capable of deauthenticating the cryptography when it enters a locked state after a predefined timeout period. Such mobile devices can be carried in a locked state in accordance with reduced physical transfer requirements based on the assurance given in the cryptographic functions.

22.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4546]

Agencies MUST ensure mobile devices are carried in a secured state when not being actively used, by:

- power off; or
- power on but pass code enabled.

Using mobile devices

22.2.6.R.01. **Rationale**

Mobile devices are portable in nature and can be easily stolen or misplaced. It is strongly advised that personnel do not leave mobile devices unattended at any time.

22.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4550]

When in use mobile devices MUST be kept under continual direct supervision.

Travelling with mobile devices

22.2.7.R.01. **Rationale**

If personnel place mobile devices or media in checked-in luggage when travelling they lose control over the devices. Such situations provide an opportunity for mobile devices to be stolen or tampered with by an attacker.

22.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4554]

When travelling with mobile devices and media, personnel MUST retain control over them at all times including by not placing them in checked-in luggage or leaving them unattended.

22.2.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4555]

Travelling personnel requested to decrypt mobile devices for inspection or from whom mobile devices are taken out of sight by border control MUST report the potential compromise of classified information or the device to an ITSM as soon as possible.