11.3. Telephones and Telephone Systems

Objective

11.3.1. Telephone systems are prevented from communicating unauthorised classified information.

Context

Scope

11.3.2. This section covers information relating to the secure use of fixed, including cordless, telephones, as well as the systems they use to communicate information.

11.3.3. 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.

11.3.4. It MUST be noted that VOIP and cellular phones have some of the same vulnerabilities as wired and cordless phones.

Rationale & Controls

Telephones and telephone systems usage policy

11.3.5.R.01. **Rationale**

All unsecure telephone networks are subject to interception. The level of expertise needed to do this varies greatly. Accidentally or maliciously revealing classified information over a public telephone networks can lead to interception.

11.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2627]

Agencies MUST develop a policy governing the use of telephones and telephone systems.

Personnel awareness

11.3.6.R.01. **Rationale**

There is a high risk of unintended disclosure of classified information when using telephones. It is important that personnel are made aware of what levels of classified information they discuss on particular telephone systems as well as the audio security risk associated with the use of telephones.

11.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2630]

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

11.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2631]

Agencies SHOULD advise personnel of the audio security risk posed by using telephones in areas where classified conversations can occur.

Visual indication

11.3.7.R.01. **Rationale**

When single telephone systems are approved to hold conversations at different classifications, alerting the user to the classification level they can speak at when using their phone will assist in the reducing the risk of unintended disclosure of classified information.

11.3.7.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2637]

Agencies permitting different levels of conversation for different types of connections MUST use telephones that give a visual indication of the classification of the connection made.

Use of telephone systems

11.3.8.R.01. **Rationale**

When classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption measures.

11.3.8.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2643]

Agencies intending to use telephone systems for the transmission of classified information MUST ensure that:

- the system has been accredited for the purpose; and
- all classified traffic that passes over external systems is appropriately encrypted.

Cordless telephones

11.3.9.R.01. **Rationale**

Cordless telephones have little or no effective transmission security, therefore should not be used for classified or sensitive communications. They also operate in an unlicensed part of the radio spectrum used for a wide range of other devices.

11.3.9.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must Not** [CID:2648]

Agencies MUST NOT use cordless telephones for classified conversations.

11.3.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2649]

Agencies SHOULD NOT use cordless telephones for classified or sensitive conversations.

Cordless telephones with secure telephony devices

11.3.10.R.01. **Rationale**

As the data between cordless handsets and base stations is not secure, cordless telephones MUST NOT be used for classified communications even if the device is connected to a secure telephony device.

11.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:2652]

Agencies MUST NOT use cordless telephones in conjunction with secure telephony devices.

Speakerphones

11.3.11.R.01. **Rationale**

Speakerphones are designed to pick up and transmit conversations in the vicinity of the device they should not be used in secure areas as the audio security risk is extremely high.

11.3.11.R.02. **Rationale**

If the agency is able to reduce the audio security risk through the use of appropriate countermeasures then an exception may be approved by the Accreditation Authority.

11.3.11.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2656]

If a speakerphone is to be used on a secure telephone system within a secure area, agencies MUST apply the following controls:

- it is located in a room rated as audio secure;
- the room is audio secure during any conversations;
- only cleared personnel involved in discussions are present in the room; and
- ensure approval for this exception is granted by the Accreditation Authority.

Off-hook audio protection

11.3.12.R.01. **Rationale**

Providing off-hook security minimises the chance of accidental classified conversation being coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat. This is normally achieved with push-to-talk (PTT) mechanisms.

11.3.12.R.02. **Rationale**

Simply providing an off-hook audio protection feature is not, in itself, sufficient. To ensure that the protection feature is used appropriately personnel will need to be made aware of the protection feature and trained in its proper use. Where PTT or some other similar functionality is

installed, the activation mechanism (such as a button or switch) must be clearly labelled.

11.3.12.R.03. **Rationale**

Many new digital desk phones control these functions through software, rather than a mechanical switch.

11.3.12.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:2661]

Agencies MUST ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

11.3.12.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2662]

Agencies MUST use push-to-talk mechanisms to meet the requirement for off-hook audio protection. PTT activation MUST be clearly labelled.

11.3.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2663]

Agencies SHOULD ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Electronic Records Retention and Voicemail

11.3.13.R.01. **Rationale**

Voicemail and other messages and communications may fall within the legal definition of electronic records. If so retention and archive requirements are prescribed.

11.3.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2666]

Agencies MUST remove unused voice mailboxes.

11.3.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2667]

Agencies MUST expire and archive or delete voicemail messages after the retention period determined by the agency's electronic records retention policy.

11.3.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2669]

Agencies SHOULD develop and implement a policy to manage the retention and disposal of such electronic records, including voicemail, email and other electronic records.