11.2. Radio frequency and infrared devices in secure areas

Objective

11.2.1. To maintain the integrity of secure areas, only approved radio frequency (RF) and infrared (IR) devices are brought into secure areas.

Context

Scope

11.2.2. This section covers information relating to the use of RF and infrared devices in secure areas. Information on the use of RF devices outside secure areas can be found in Chapter 21 - Distributed working.

11.2.3. RF devices include any transmitter on any frequency, including mobile phones, cordless phones, Bluetooth, Wi-Fi, RFID and other similar devices. Requirements for Bluetooth devices are described in section 11.1

11.2.4. IR devices transmit data over variable distances using light waves; examples are infrared cameras; night vision devices; infrared computer ports; and remote controls.

11.2.5. A secure area, in the context of the NZISM, is defined as any area, room, group of rooms, building or installation that processes, stores or communicates information classified CONFIDENTIAL, SECRET, TOP SECRET or any compartmented or caveated information at these classifications. A secure area may include a Sensitive Compartmented Information Facility (SCIF).

The physical security requirements for such areas are specified in the Protective Security Requirements (PSR) Security Zones.

Exemptions for the use of RF devices

11.2.6. At the discretion of the Accreditation Authority, RF devices can be used in a secure area provided they cannot communicate or compromise classified information.

Exemptions for the use of Medical devices

11.2.7. At the discretion of the Accreditation Authority, medical devices with RF transmitters and/or receivers can be used in secure areas provided they cannot communicate or compromise classified information.

Exemptions for the use of IR and laser devices

11.2.8. At the discretion of the Accreditation Authority, IR and laser devices can be used in a secure area provided they cannot communicate or compromise classified information.

References

11.2.9. References are available at the following source:

Reference	Publisher	Title
NIST 800-121, Rev.2, May 2017 (INCLUDES UPDATES AS OF 1-19-2022)	NIST	Guide to Bluetooth Security (nist.gov)

PSR references

11.2.10. 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

RF devices in secure areas

11.2.11.R.01. **Rationale**

RF devices pose security threat as they are capable of picking up and transmitting classified background conversations. Furthermore, many RF devices can connect to IT equipment and act as unauthorised data storage devices or bridge "air gaps".

11.2.11.C.01 **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:2497]

Agencies MUST prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

11.2.11.C.02 **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2498]

Agencies SHOULD prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

RF controls in secure areas

11.2.12.R.01. **Rationale**

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

11.2.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2504]

Agencies SHOULD limit the effective range of communications outside the agency's area of control by:

- minimising the output power level of wireless devices;
- RF shielding; and
- Physical layout and separation.

Detecting RF devices in secure areas

11.2.13.R.01. **Rationale**

As RF devices are prohibited in secure areas, agencies should deploy technical measures to detect and respond to the unauthorised use of such devices.

11.2.13.C.01 **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Should** [CID:2501]

Agencies SHOULD deploy measures to detect and respond to active RF devices within secure areas.

Pointing devices

11.2.14.R.01. **Rationale**

Wireless RF or IR pointing devices can pose an emanation security risk as well as introduce vulnerabilities to classified IT equipment and/or systems.

11.2.14.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must Not** [CID:2483]

Wireless RF or IR pointing devices MUST NOT be used in secure areas unless approved by the Accreditation Authority and appropriate RF or IR mitigations are implemented.

IR devices in secure areas

11.2.15.R.01. **Rationale**

When using IR devices with CONFIDENTIAL, SECRET or TOP SECRET systems, IR mitigations including opaque curtains and/or IR window films are

acceptable. Line of sight must be managed for direct and reflected transmissions. While infrared transmissions are generally designed for short range (5 to 10 metres) manufacturing and design variations and some environmental conditions can amplify and reflect infrared over much greater distances.

11.2.15.R.02. **Rationale**

When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are NOT acceptable as a method of permanently blocking infrared transmissions. While infrared transmissions are generally designed for short range (5 to 10 metres) manufacturing and design variations and some environmental conditions can amplify and reflect infrared over much greater distances.

11.2.15.C.01. **Control System Classifications(s): Secret, Confidential; Compliance: Must Not** [CID:2487]

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple infrared keyboards at different classifications in the same area;
- other infrared devices to be brought into line of sight of the keyboard or its receiving device/port; and
- infrared keyboards to be operated in areas with unprotected windows.

11.2.15.C.02. **Control System Classifications(s): Top Secret; Compliance: Must Not** [CID:2488]

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple infrared keyboards at different classifications in the same area;
- other infrared devices within the same area; and
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

11.2.15.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2489]

Agencies using IR devices SHOULD ensure that the IR receiver/port is positioned to prevent line of sight from the secure area boundary.