10.4. Cable Management for Shared Non-Government Facilities

Objective

10.4.1. Cable management systems are implemented in shared non-government facilities to minimise risks to data and information.

Context

Scope

10.4.2. This section provides specific requirements for cabling installed in facilities shared by agencies and non-government organisations. This section is to be applied in addition to common requirements for cabling as outlined in Section 10.1 - Cable Management Fundamentals section.

Applicability of controls within this section

10.4.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Rationale & Controls

Use of fibre optic cabling

10.4.4.R.01. **Rationale**

Fibre optic cabling is essential in a shared non-government facility. Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared non-government facility where an agency's controls may have a limited effect outside the agency controlled area.

10.4.4.R.02. **Rationale**

Fibre optic cable is more difficult to tap than copper cabling and anti-tampering monitoring can be employed to detect tampering.

10.4.4.R.03. **Rationale**

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

10.4.4.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2335]

In TOP SECRET areas, agencies MUST use fibre optic cabling.

10.4.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2336]

Agencies SHOULD use fibre optic cabling.

Cabling inspection

10.4.5.R.01. **Rationale**

In a shared non-government facility, it is imperative that cabling systems be inspectable for tampering and damage on a regular basis particularly where higher threat levels exist or where threats are unknown.

10.4.5.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2340]

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.4.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2341]

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

Cables sharing a common reticulation system

10.4.6.R.01. **Rationale**

In a shared non-government facility, tighter controls are placed on sharing reticulation systems as the threats attributable to tampering and damage are increased.

10.4.6.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2344]

In TOP SECRET areas, approved cable groups can share a common reticulation system but MUST have either a dividing partition or a visible gap between the differing cable groups.

10.4.6.C.02. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2345]

TOP SECRET cabling MUST run in a non-shared, enclosed reticulation system.

10.4.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2346]

Approved cable groups can share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups.

Enclosed cable reticulation systems

10.4.7.R.01. **Rationale**

In a shared non-government facility, TOP SECRET cabling is enclosed in a sealed reticulation system to prevent access and control cable management.

10.4.7.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2349]

In TOP SECRET areas, the front covers for conduits and cable trays in floors, ceilings and of associated fittings MUST be clear plastic or be inspectable and have tamper proof seals fitted.

10.4.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2350]

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings SHOULD be clear plastic or be inspectable and have tamper proof seals fitted.

Cabling in walls or party walls

10.4.8.R.01. **Rationale**

In a shared non-government facility, cabling run correctly in walls allows for neater installations facilitating separation and inspectability. Controls are more stringent than in a non-shared facility or a shared government facility.

10.4.8.R.02. **Rationale**

A party wall is a wall shared with an unclassified area where there is no control over access. In a shared non-government facility, cabling is not allowed in a party wall. An inner wall can be used to run cabling where the area is sufficient for inspection of the cabling.

10.4.8.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:2354]

Cabling MUST NOT run in a party wall.

Sealing reticulation systems

10.4.9.R.01. **Rationale**

In a shared non-government facility, where the threats of access to cable reticulation systems is increased, GCSB endorsed anti-tamper seals are required to provide evidence of any tampering or illicit access.

10.4.9.R.02. **Rationale**

In a shared non-government facility, all conduit joints and wall penetrations are sealed with a visible smear of glue or sealant to prevent access to cabling.

10.4.9.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2358]

Agencies MUST use GCSB endorsed tamper evident seals to seal all removable covers on reticulation systems, including:

- conduit inspection boxes;

- outlet and junction boxes; and
- T-pieces.

10.4.9.C.02. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2359]

Tamper evident seals MUST be uniquely identifiable and a register kept of their unique number and location.

10.4.9.C.03. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2360]

Conduit joints MUST be sealed with glue or sealant.

10.4.9.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2361]

Conduit joints SHOULD be sealed with glue or sealant.

Wall penetrations

10.4.10.R.01. **Rationale**

A cable wall penetration into a lesser-classified area requires the integrity of the classified area be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure area.

10.4.10.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:2365]

Wall penetrations that exit into a lower classified area, cabling MUST be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

10.4.11.R.01. **Rationale**

In a shared non-government facility, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means. The addition of a UPS is required to maintain availability of the TOP SECRET systems.

10.4.11.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:2368]

Secure facilities MUST have a power distribution board located within the secure area and supply UPS power all equipment.

Power Filters

10.4.12.R.01. **Rationale**

Power filters are used to provide filtered (clean) power and reduce opportunity for technical attacks. Refer to 10.1.32 or consult the GCSB for technical advice.

10.4.12.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2371]

Power filters MUST be used to provide filtered (clean) power and reduce opportunity for technical attacks.

Equipment Cabinet separation

10.4.13.R.01. **Rationale**

A visible gap between equipment cabinets will make any cross-cabling obvious and will simplify inspections for unauthorised or compromising changes.

10.4.13.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:2374]

Equipment cabinets MUST have a visible gap or non-conductive isolator between cabinets of different classifications.

10.4.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2375]

There SHOULD be a visible inspectable gap or non-conductive isolator between equipment cabinets of different classifications.