10.2. Cable Management for Non-Shared Government Facilities

Objective

10.2.1. Cable management systems in non-shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.2.2. This section provides specific requirements for cabling installed in **non-shared** Government facilities.

- A **non-shared** facility is a facility occupied **solely** by a single agency.
- A **shared** facility is a facility occupied by **more than one** agency. A shared facility should have stricter physical and technical security controls than a non-shared facility.

10.2.3. This section is to be applied in addition to common requirements for cabling as outlined in the Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

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

References

10.2.5. Further references can be found at:

Reference	Title	Publisher	Source
NZCSS 400	**New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)**	GCSB	GCSB CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012	**Electrical Installations (Known as the Australia/New Zealand Wiring Rules**	Standards NZ	https://standards.govt.nz/

Rationale & Controls

Cabling Inspection

10.2.6.R.01. **Rationale**

Regular inspections of cable installations are necessary to detect any unauthorised or malicious tampering or cable degradation.

10.2.6.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2270]

In TOP SECRET areas or zones, all cabling MUST be inspectable at a minimum of five-metre intervals.

10.2.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2271]

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

Cables sharing a common reticulation system

10.2.7.R.01. **Rationale**

Laying cabling in a neat and controlled manner, observing separation requirements, allows for inspections and reduces the need for individual cable trays for each classification.

10.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2274]

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

Cabling in walls

10.2.8.R.01. **Rationale**

Cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements.

10.2.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2277]

Flexible or plastic conduit SHOULD be used in walls to run cabling from cable trays to wall outlets.

Cabinet separation

10.2.9.R.01. **Rationale**

Having a definite gap between cabinets allows for ease of inspections for any unauthorised or malicious cabling or cross patching.

10.2.9.C.01. **Control System Classifications(s): Top Secret; Compliance: Should** [CID:2280]

TOP SECRET cabinets SHOULD have a visible inspectable gap between themselves and lower classified cabinets.

Power Filters

10.2.10.R.01. **Rationale**

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.2.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:5902]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.