



# Information Security Manual

Published: 1 March 2024

## Guidelines for Communications Infrastructure

### Cabling infrastructure

#### Applicability

This section is only applicable to facilities located within Australia.

#### Shared facilities

In addition to common controls, this section provides additional controls for shared facilities, such as a single floor, or part of a floor, within a multi-tenanted building.

#### Cables and structured cabling systems

For the purposes of this section, a cable is defined as any fibre optic or copper material housed within a protective sheath for the purposes of transmitting data or control signals from one point in a facility to another. Each cable will form part of a structured cabling system and will need to comply with the Australian Standards associated with that system. In addition to network communications and data systems, some common building management structured cabling systems found within facilities are:

- fire control and sensor systems
- security control and surveillance systems
- lighting control systems
- access control systems
- voice and emergency telephony systems
- emergency control alert systems.

#### Cable sheaths and conduits

A cable's protective sheath is not considered to be a conduit.

#### Cable connector types

The same cable connector types can be used for all systems within a facility regardless of their sensitivity or classification.

## Cabling infrastructure standards

Cabling infrastructure should be installed by an endorsed cable installer to the relevant Australian Standards to ensure personnel safety and system availability.

**Control: ISM-0181; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A**

*Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.*

## Use of fibre-optic cables

Fibre-optic cables do not produce, nor are influenced by, electromagnetic emanations; thereby offering the highest degree of protection from electromagnetic emanation effects.

**Control: ISM-1111; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A**

*Fibre-optic cables are used for cabling infrastructure instead of copper cables.*

## Cable register

Developing, implementing, maintaining and regularly verifying cable registers assists installers and inspectors, with the help of floor plan diagrams, to trace cables for malicious or accidental changes or damage. In doing so, cable registers should track all cabling changes throughout the life of a system.

**Control: ISM-0211; Revision: 7; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

*A cable register is developed, implemented, maintained and verified on a regular basis.*

**Control: ISM-0208; Revision: 6; Updated: Jun-21; Applicability: All; Essential Eight: N/A**

*A cable register contains the following for each cable:*

- *cable identifier*
- *cable colour*
- *sensitivity/classification*
- *source*
- *destination*
- *location*
- *seal numbers (if applicable).*

## Floor plan diagrams

Floor plan diagrams that are developed using computer-aided design and drafting software, and use alphanumeric grid referencing, can provide an accurate scaled view for each floor and are critical to ensuring that cabling infrastructure components can be easily located by installers and inspectors. In doing so, floor plan diagrams should track all cabling infrastructure changes throughout the life of a system.

**Control: ISM-1645; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

*Floor plan diagrams are developed, implemented, maintained and verified on a regular basis.*

**Control: ISM-1646; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A**

*Floor plan diagrams contain the following:*

- *cable paths (including ingress and egress points between floors)*
- *cable reticulation system and conduit paths*
- *floor concentration boxes*
- *wall outlet boxes*
- *network cabinets.*

## Cable labelling processes and procedures

Well documented cable labelling processes and procedures can make cable verification and fault finding easier.

**Control:** ISM-0206; **Revision:** 7; **Updated:** Dec-22; **Applicability:** All; **Essential Eight:** N/A

*Cable labelling processes, and supporting cable labelling procedures, are developed, implemented and maintained.*

### Labelling cables

Labelling cables with the correct source and destination details minimises the likelihood of cross-patching and aids in fault finding and configuration management.

**Control:** ISM-1096; **Revision:** 2; **Updated:** Oct-19; **Applicability:** All; **Essential Eight:** N/A

*Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.*

### Labelling building management cables

All facilities will contain structured cabling systems to support building management and control functions. As Australian Standards require some structured cabling systems to use specified colours, such as red for fire control systems, it is important that all building management cables are appropriately labelled.

**Control:** ISM-1639; **Revision:** 0; **Updated:** Mar-21; **Applicability:** All; **Essential Eight:** N/A

*Building management cables are labelled with their purpose in black writing on a yellow background, with a minimum size of 2.5 cm x 1 cm, and attached at five-metre intervals.*

### Labelling cables for foreign systems in Australian facilities

Labelling cables for foreign systems in Australian facilities helps prevent unintended cross-patching of Australian and foreign systems.

**Control:** ISM-1640; **Revision:** 0; **Updated:** Mar-21; **Applicability:** All; **Essential Eight:** N/A

*Cables for foreign systems installed in Australian facilities are labelled at inspection points.*

### Cable colours

To avoid confusion, it is important that, regardless of the type of cabling involved, a consistent cable colour is used. Furthermore, the use of designated cable colours can provide an easy way to distinguish cables for SECRET and TOP SECRET systems from cables for other systems. For example, while SECRET and TOP SECRET cables have designated cable colours, cables for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, cable colours for other systems, such as OFFICIAL: Sensitive and PROTECTED systems, may use the same colour, such as blue.

**Control:** ISM-1820; **Revision:** 0; **Updated:** Mar-23; **Applicability:** All; **Essential Eight:** N/A

*Cables for individual systems use a consistent colour.*

**Control:** ISM-0926; **Revision:** 10; **Updated:** Sep-23; **Applicability:** OS, P; **Essential Eight:** N/A

*OFFICIAL: Sensitive and PROTECTED cables are coloured neither salmon pink nor red.*

**Control:** ISM-1718; **Revision:** 1; **Updated:** Mar-23; **Applicability:** S; **Essential Eight:** N/A

*SECRET cables are coloured salmon pink.*

**Control:** ISM-1719; **Revision:** 1; **Updated:** Mar-23; **Applicability:** TS; **Essential Eight:** N/A

*TOP SECRET cables are coloured red.*

### Cable colour non-conformance

In certain circumstances it may not be possible to use the correct colour for SECRET or TOP SECRET cables. In such cases, an organisation should band such cables with the appropriate colour and ensure that the cable bands are easily visible at inspection points. In doing so, it is important that cable bands are robust enough to stand the test of time. Examples of appropriate cable bands include stick-on coloured labels, colour heat shrink, coloured ferrules or short lengths of banded conduit.

**Control: ISM-1216; Revision: 3; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

*SECRET and TOP SECRET cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.*

## **Cable inspectability**

The ability to inspect cabling infrastructure is necessary to detect illicit tampering or degradation. Note, this does not necessarily mean that cables need to be fully visible all the time. Rather, cable inspectability can still be achieved as long as cables can be viewed and inspected through the easy removal of ceiling, floor or wall panels or manholes.

**Control: ISM-1112; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Cables are inspectable at a minimum of five-metre intervals.*

**Control: ISM-1119; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Cables in TOP SECRET areas are fully inspectable for their entire length.*

## **Common cable bundles and conduits**

In some circumstances, cables for different systems can be bundled together or run in a common conduit in order to reduce costs, such as cables for OFFICIAL: Sensitive and PROTECTED systems.

**Control: ISM-0187; Revision: 8; Updated: Mar-23; Applicability: S; Essential Eight: N/A**

*SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.*

**Control: ISM-1821; Revision: 0; Updated: Mar-23; Applicability: TS; Essential Eight: N/A**

*TOP SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.*

## **Common cable reticulation systems**

When cable reticulation systems are used for more than one cable bundle or conduit, it is important that there is a dividing partition or visible gap between cable bundles and conduits to facilitate easier cable inspection.

**Control: ISM-1114; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A**

*Cable bundles or conduits sharing a common cable reticulation system have a dividing partition or visible gap between each cable bundle and conduit.*

## **Enclosed cable reticulation systems**

In shared facilities, cables should be enclosed in a sealed cable reticulation system to prevent access and enhance cable management.

**Control: ISM-1130; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*In shared facilities, cables are run in an enclosed cable reticulation system.*

## **Covers for enclosed cable reticulation systems**

In shared facilities, clear covers on enclosed cable reticulation systems are a convenient method of maintaining inspection requirements. Having clear covers face inwards increases their inspectability.

**Control: ISM-1164; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*In shared facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.*

## **Sealing cable reticulation systems and conduits**

In shared facilities, uniquely identifiable Security Construction and Equipment Committee (SCEC)-approved tamper-evident seals should be used to provide evidence of any tampering or illicit access to TOP SECRET cable reticulation systems. In addition, TOP SECRET conduits should be sealed with a visible smear of conduit glue to prevent access.

**Control: ISM-0195; Revision: 7; Updated: Jun-22; Applicability: TS; Essential Eight: N/A**

*In shared facilities, uniquely identifiable SCEC-approved tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.*

**Control:** ISM-0194; **Revision:** 3; **Updated:** Dec-21; **Applicability:** TS; **Essential Eight:** N/A

*In shared facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and TOP SECRET conduits connected by threaded lock nuts.*

## Labelling conduits

Labels for TOP SECRET conduits should be of sufficient size and colour to allow for easy identification.

**Control:** ISM-0201; **Revision:** 3; **Updated:** Mar-21; **Applicability:** TS; **Essential Eight:** N/A

*Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.*

## Cables in walls

Cables run correctly in walls allow for neater installations while maintaining separation and inspection requirements.

**Control:** ISM-1115; **Revision:** 4; **Updated:** Dec-19; **Applicability:** All; **Essential Eight:** N/A

*Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.*

## Cables in party walls

In shared facilities, TOP SECRET cables are not run in party walls. However, an inner wall can be used to run TOP SECRET cables where sufficient space exists for their inspection.

**Control:** ISM-1133; **Revision:** 3; **Updated:** Dec-21; **Applicability:** TS; **Essential Eight:** N/A

*In shared facilities, TOP SECRET cables are not run in party walls.*

## Wall penetrations

Penetrating a wall between a TOP SECRET area and a lower classified area requires the integrity of the TOP SECRET area to be maintained. In such scenarios, TOP SECRET cables should be encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.

**Control:** ISM-1122; **Revision:** 2; **Updated:** Dec-21; **Applicability:** TS; **Essential Eight:** N/A

*Where wall penetrations exit a TOP SECRET area into a lower classified area, TOP SECRET cables are encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.*

## Wall outlet boxes

Wall outlet boxes are the main method of connecting cabling infrastructure to workstations. They allow the management of cables and the types of connectors allocated to various systems.

**Control:** ISM-1105; **Revision:** 4; **Updated:** Mar-23; **Applicability:** S, TS; **Essential Eight:** N/A

*SECRET and TOP SECRET wall outlet boxes contain exclusively SECRET or TOP SECRET cables.*

## Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment to the wrong wall outlet box. In cases where a wall outbox contains cables for different systems, each connector should be individually labelled.

**Control:** ISM-1095; **Revision:** 5; **Updated:** Dec-21; **Applicability:** All; **Essential Eight:** N/A

*Wall outlet boxes denote the systems, cable identifiers and wall outlet box identifier.*

## Wall outlet box colours

The use of designated wall outlet box colours can provide an easy way to distinguish wall outlet boxes for SECRET and TOP SECRET systems from wall outlet boxes for other systems. For example, while SECRET and TOP SECRET wall outlet boxes have designated wall outlet box colours, wall outlet boxes for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, wall outlet box colours for other systems, such as OFFICIAL:

Sensitive and PROTECTED systems, may use the same colour, such as blue. Ideally, wall outlet boxes should be the same colour that is used for associated cabling.

**Control: ISM-1822; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A**  
*Wall outlet boxes for individual systems use a consistent colour.*

**Control: ISM-1107; Revision: 6; Updated: Sep-23; Applicability: OS, P; Essential Eight: N/A**  
*OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.*

**Control: ISM-1720; Revision: 0; Updated: Dec-21; Applicability: S; Essential Eight: N/A**  
*SECRET wall outlet boxes are coloured salmon pink.*

**Control: ISM-1721; Revision: 0; Updated: Dec-21; Applicability: TS; Essential Eight: N/A**  
*TOP SECRET wall outlet boxes are coloured red.*

## Wall outlet box covers

Transparent wall outlet box covers allow for inspection of cable cross-patching and tampering.

**Control: ISM-1109; Revision: 3; Updated: Dec-19; Applicability: All; Essential Eight: N/A**  
*Wall outlet box covers are clear plastic.*

## Fly lead installation

Keeping the lengths of TOP SECRET fibre-optic fly leads to a minimum prevents clutter around desks, prevents damage, and reduces the chance of cross-patching and tampering. If lengths become excessive, TOP SECRET fibre-optic fly leads should be treated as cabling infrastructure and run in TOP SECRET conduit or fixed infrastructure, such as desk partitioning.

**Control: ISM-0218; Revision: 6; Updated: Dec-21; Applicability: TS; Essential Eight: N/A**  
*If TOP SECRET fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to ICT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the ICT equipment end with the wall outlet box's identifier.*

## Connecting cable reticulation systems to cabinets

Controlling the routing from cable reticulation systems to cabinets can assist in preventing unauthorised modifications and tampering while also providing easy inspection of cables.

**Control: ISM-1102; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**  
*Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.*

**Control: ISM-1101; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**  
*In TOP SECRET areas, cable reticulation systems leading into cabinets in server rooms or communications rooms are terminated as close as possible to the cabinet.*

**Control: ISM-1103; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**  
*In TOP SECRET areas, cable reticulation systems leading into cabinets not in server rooms or communications rooms are terminated at the boundary of the cabinet.*

## Terminating cables in cabinets

Having individual or divided cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

**Control: ISM-1098; Revision: 5; Updated: Mar-23; Applicability: S; Essential Eight: N/A**  
*SECRET cables are terminated in an individual cabinet; or for small systems, a cabinet with a division plate between any SECRET cables and non-SECRET cables.*

**Control: ISM-1100; Revision: 1; Updated: Sep-18; Applicability: TS; Essential Eight: N/A**  
*TOP SECRET cables are terminated in an individual TOP SECRET cabinet.*

## Terminating cables on patch panels

Terminating SECRET and TOP SECRET cables on different patch panels in cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

**Control:** ISM-0213; **Revision:** 4; **Updated:** Mar-23; **Applicability:** S, TS; **Essential Eight:** N/A  
*SECRET and TOP SECRET cables are terminated on their own individual patch panels.*

## Physical separation of cabinets and patch panels

Physical separation between TOP SECRET systems and non-TOP SECRET systems reduces the chance of cross-patching, thereby the possibility of unauthorised personnel gaining access to TOP SECRET systems.

**Control:** ISM-0216; **Revision:** 3; **Updated:** Mar-23; **Applicability:** TS; **Essential Eight:** N/A  
*TOP SECRET patch panels are installed in individual TOP SECRET cabinets.*

**Control:** ISM-0217; **Revision:** 5; **Updated:** Mar-23; **Applicability:** TS; **Essential Eight:** N/A  
*Where spatial constraints demand non-TOP SECRET patch panels be installed in the same cabinet as a TOP SECRET patch panel:*

- *a physical barrier in the cabinet is provided to separate patch panels*
- *only personnel holding a Positive Vetting security clearance have access to the cabinet*
- *approval from the TOP SECRET system's authorising officer is obtained prior to installation.*

**Control:** ISM-1116; **Revision:** 4; **Updated:** Mar-23; **Applicability:** TS; **Essential Eight:** N/A  
*A visible gap exists between TOP SECRET cabinets and non-TOP SECRET cabinets.*

## Audio secure rooms

Audio secure rooms are designed to prevent audio conversations from being overheard. The Australian Security Intelligence Organisation should be consulted before any modifications are made to TOP SECRET audio secure rooms.

**Control:** ISM-0198; **Revision:** 3; **Updated:** Dec-21; **Applicability:** TS; **Essential Eight:** N/A  
*When penetrating a TOP SECRET audio secure room, the Australian Security Intelligence Organisation is consulted and all directions provided are complied with.*

## Power reticulation

It is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

**Control:** ISM-1123; **Revision:** 3; **Updated:** Dec-21; **Applicability:** TS; **Essential Eight:** N/A  
*A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.*

## Further information

[Australian cabling standards and regulations](#) can be obtained from the Australian Communications and Media Authority.

Further information on SCEC-approved tamper-evident seals can be found on the SCEC's [Security Equipment Evaluated Products List](#).

Further information on audio secure rooms can be found in the Department of Home Affairs' [Protective Security Policy Framework](#), [Physical security for entity resources](#) policy.

## Emanation security

### Electromagnetic interference/electromagnetic compatibility standards

All ICT equipment used by systems will need to meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

**Control: ISM-0250; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*ICT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.*

## **Emanation security doctrine**

The Australian Signals Directorate (ASD) specifies additional emanation security requirements in Australian Communications Security Instructions that must be complied with. Such requirements supplement these guidelines and, where conflicts occur, take precedence.

**Control: ISM-1884; Revision: 0; Updated: Dec-23; Applicability: OS, P, S, TS; Essential Eight: N/A**

*Emanation security doctrine produced by ASD for the management of emanation security matters is complied with.*

## **Emanation security threat assessments**

Obtaining advice from ASD on emanation security threats is vital to protecting SECRET and TOP SECRET systems, both inside and outside of Australian borders. In particular, this can assist in preventing SECRET and TOP SECRET systems from emanating compromising signals, which if intercepted and analysed, could lead to serious consequences. Note, the implementation of such advice is in addition to, and not a replacement for, industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

In conducting emanation security threat assessments, it is important that they are sought by system owners as early as possible in a system's life cycle as development timeframes and costs will be much greater if changes have to be made to systems once they have been designed and implemented.

On completion of emanation security threat assessments, system owners will receive a TEMPEST requirements statement that contains recommended actions to be taken to reduce emanation security risks. In doing so, any recommendations not implemented by system owners will need to be accepted by a system's authorising officer.

**Control: ISM-1137; Revision: 5; Updated: Dec-23; Applicability: S, TS; Essential Eight: N/A**

*System owners deploying SECRET or TOP SECRET systems within fixed facilities contact ASD for an emanation security threat assessment.*

**Control: ISM-0248; Revision: 8; Updated: Dec-23; Applicability: OS, P; Essential Eight: N/A**

*System owners deploying OFFICIAL: Sensitive or PROTECTED systems with radio frequency transmitters (including any wireless capabilities) that will be located within 20 meters of SECRET or TOP SECRET systems contact ASD for an emanation security threat assessment.*

**Control: ISM-0249; Revision: 6; Updated: Dec-23; Applicability: S, TS; Essential Eight: N/A**

*System owners deploying SECRET or TOP SECRET systems in mobile platforms, or as a deployable capability, contact ASD for an emanation security threat assessment.*

**Control: ISM-0246; Revision: 5; Updated: Dec-23; Applicability: OS, P, S, TS; Essential Eight: N/A**

*When an emanation security threat assessment is required, it is sought as early as possible in a system's life cycle.*

**Control: ISM-1885; Revision: 0; Updated: Dec-23; Applicability: OS, P, S, TS; Essential Eight: N/A**

*Recommended actions contained within TEMPEST requirements statements issued for systems are implemented by system owners.*

## **Further information**

Further information on ASD's [Emanation Security Program](#), including a list of certified emanation security providers, is available from ASD.