8.3. Network Infrastructure

Objective

8.3.1. Network infrastructure is protected by secure facilities and the use of encryption technologies.

Context

Scope

8.3.2. This section covers information relating to the physical security of network infrastructure. Information relating to servers, network devices and IT equipment can be found in other sections of this chapter. Additionally, information on using encryption for infrastructure in unsecure areas can be found in Section 17.1 - Cryptographic Fundamentals.

Rationale & Controls

Network infrastructure in secure areas

8.3.3.R.01. **Rationale**

Network infrastructure is considered to process information being communicated across it and as such needs to meet the minimum physical security requirements for processing classified information as specified in the PSR Policy Framework - Physical security, and supporting document.

8.3.3.R.02. **Rationale**

The physical security requirements for network infrastructure can be lowered if encryption is being applied to classified information communicated over the infrastructure (i.e. data in transit encryption). Note this does NOT change the classification of the data itself, only the physical protection requirements.

8.3.3.R.03. **Rationale**

It is important to note that physical controls do not provide any protection against malicious software or other malicious entities that may be residing on or have access to the system.

8.3.3.R.04. **Rationale**

If classified information being communicated over the infrastructure is not encrypted the malicious entry can capture, corrupt or modify the traffic to assist in furthering any attempts to exploit the network and the information being communicated across it.

8.3.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1373]

Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.

8.3.3.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1374]

Agencies communicating classified information over infrastructure in secure areas SHOULD encrypt their information with at least an Approved Cryptographic Protocol. See Section 17.3 – Approved Cryptographic Protocols.

Protecting network infrastructure

8.3.4.R.01. **Rationale**

In order to prevent tampering with patch panels, fibre distribution panels and structured wiring, any such enclosures need to be placed within at least lockable commercial cabinets. Furthermore, keys for such cabinets should not be remain in locks as this defeats the purpose of using lockable commercial cabinets in the first place.

8.3.4.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1377]

Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.

8.3.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1378]

Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.

Network infrastructure in unsecure areas

8.3.5.R.01. **Rationale**

As agencies lose control over classified information when it is communicated over unsecure public network infrastructure or over infrastructure in unsecure areas they MUST ensure that it is encrypted to a sufficient level that if it was captured that it would be sufficiently difficult to determine the original information from the encrypted information.

8.3.5.R.02. **Rationale**

Encryption does not change the class level of the information itself but allows reduced handling requirements to be applied.

8.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1382]

Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.