18.6. Peripheral (KVM) Switches

Objective

18.6.1. An evaluated peripheral switch is used when sharing keyboards, monitors and mice or other user interface devices, between different systems.

Context

Scope

18.6.2. This section covers information relating specifically to the use of keyboard/video/mouse (KVM) switches.

18.6.3. It is important to recognise that any cross-connection of system must be carefully controlled in order not to compromise trust zones. The principles of separation and segregation must be applied. These principles are discussed in Section 22.1 – Cloud Computing and Section 22.2 – Virtualisation.

18.6.4. Cross-connection of system may also functionally create a gateway, whether or not it meets the technical definition of gateways. It is important to refer to Section 19.1 – Gateways and Section 19.2 – Cross Domain Solutions.

Peripheral switches with more than two connections

18.6.5. If the peripheral switch has more than two systems connected then the level of assurance needed is determined by the highest and lowest of the classifications involved.

Electrical Safety

18.6.6. Electrical safety is paramount. Cross-connecting systems may create ground loops if different power sources are used for different elements of the computer system. This may result in catastrophic failure if power supplies connected to different phases are cross-connected.

Product Assurance

18.6.7. Product assurance is discussed in Chapter 12- Product Security It is important to note the role of the Common Criteria, the related CCRA and the use of assurance levels in determining product assurance. chapter 12 also provides essential reference to assurance levels, evaluation levels and defines high assurance as shown in the table 18.6.8 Assurance requirements.

Rationale & Controls

Assurance requirements

18.6.8.R.01. **Rationale**

When accessing multiple systems through a peripheral switch it is important that sufficient assurance is available in the operation of the switch to ensure that information does not accidently pass between the connected systems.

18.6.8.R.02. **Rationale**

It is important to maintain the integrity of Trust Zones and adhere to the principles of separation and segregation in order to avoid inadvertently compromising Trust Zones – even if they are at the same level of classification.

18.6.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4051]

Agencies accessing a classified system and a less classified system via a peripheral switch MUST use an evaluated product with a level of assurance as indicated in the table below.

High System	Low system / Alternate Trust Domain	Required Level of Assurance
RESTRICTED	UNCLASSIFIED	EAL2 or PP
CONFIDENTIAL	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
TOP SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
	TOP SECRET	high assurance

Assurance requirements for NZEO systems

18.6.9.R.01. **Rationale**

NZEO systems are particularly sensitive. Additional security measures need to be put in place when connecting them to other systems.

18.6.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4058]

Agencies accessing a system containing NZEO information and a system of the same classification that is not accredited to process NZEO information, MUST use an evaluated product with an EAL2 (or higher) or a PP level of assurance.

Cross-Connecting Systems with a device other than a KVM

18.6.10.R.01. **Rationale**

Cross-connecting systems with any device other than a KVM approved gateway or an approved cross-domain solution may be high risk, may compromise the integrity of Trust Zones, and may create an electrical hazard.

18.6.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4066]

Cross-connection of security domains and Trust Zones MUST be enabled through an approved KVM, Gateway or Cross-Domain solution only.

High system	Low system/ Alternate Trust Domain	Level of assurance
RESTRICTED & all lower classifications	UNCLASSIFIED	EAL2 or PP
CONFIDENTIAL	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
TOP SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
	TOP SECRET	high assurance