

**UNCLASSIFIED**



# **Government Communications Security Bureau**

## **GOOD PRACTICE GUIDE FOR DESKTOP KVM SWITCH INSTALLATION AND USE**

**December 2009**

### **WARNING**

**This document is the property of the New Zealand Government and contains official information protected by law. Unauthorised disclosure or use of the material contained herein is a criminal offence.**

**New Zealand Government**

**UNCLASSIFIED**

**UNCLASSIFIED**

**Intentionally Blank**

**UNCLASSIFIED**

# UNCLASSIFIED

## FOREWORD

### Introduction

1. The Government Communications Security Bureau (GCSB) produces Good Practice Guides (GPGs) to provide guidance to New Zealand Government Departments on specific aspects of Information Assurance (IA) in order to help manage risk effectively.

### Security

2. Holders of this document are cautioned that it contains information affecting New Zealand's security. This publication must be handled in accordance with Security in the Government Sector (SIGS). The recipient department or agency assumes responsibility for control of all classified publications held.

### Format

3. While this document may be delivered in electronic form it is formatted for printing as a booklet to provide the intended audience with a physical on-job reference. Please consider the environment before printing.

### Customer Feedback

4. GCSB welcomes feedback and encourages readers to inform GCSB of their experiences, good or bad in the use of this document or pertaining to the subject of this document. GCSB would especially like to know about any inconsistencies and ambiguities. Your comments should be submitted through command channels to the Director, GCSB.

Bruce Ferguson  
Director, GCSB

December 2009

**UNCLASSIFIED**

**Intentionally Blank**

**UNCLASSIFIED**

# UNCLASSIFIED

## Table of Contents

<b>Executive Summary</b> .....	<b>5</b>
<b>Purpose</b> .....	<b>5</b>
<b>Key Words</b> .....	<b>5</b>
<b>Common Configuration</b> .....	<b>7</b>
<b>Principles</b> .....	<b>8</b>
<b>Risks</b> .....	<b>9</b>
<b>Controls</b> .....	<b>10</b>
<b>Switching requirements</b> .....	<b>12</b>
Matrix of KVM Assurance Levels .....	12
<b>Installation requirements</b> .....	<b>13</b>
<b>Further Guidance</b> .....	<b>13</b>
<b>Annex A</b> .....	<b>A-1</b>
Plain English KVM Installation Guidelines .....	A-1
<b>Annex B</b> .....	<b>B-1</b>
KVM User Best Practice Guidelines .....	B-1

**UNCLASSIFIED**

**Intentionally Blank**

**UNCLASSIFIED**

# UNCLASSIFIED

## Executive Summary

1. A Keyboard-Video-Mouse switch (KVM) conserves desk-space by allowing an operator using a single keyboard, display device (video monitor) and mouse combination to switch as required between two (or more) systems/networks while preserving the integrity of information on individual networks.
2. This guide is specific to hardware desktop (peripheral) KVM electronic switches employed by New Zealand Government Departments and covers the selection, installation and use of hardware KVM electronic switches to control co-located multiple computers on disparate networks up to TOP SECRET from a single keyboard, display device and mouse.
3. This guide establishes requirements for the selection, installation and use of KVM to ensure that:
  - a. Switching between disparate networks (e.g. a private or classified network and another classified network or the Internet) is achieved as securely as possible;
  - b. Electronic attack (eA) or passive electronic eavesdropping against the private or classified network is not facilitated by the use of the KVM;
  - c. Precautions are in place to avoid classified information being placed on an Internet connected network, for example by inadvertent selection of the incorrect network at the KVM;
  - d. Systems interconnected via KVM are correctly configured; and
  - e. ICT system administrators and users of KVM understand their responsibilities.
4. Each KVM product and its operation are described in the associated user manuals supplied with the equipment.

## Purpose

5. This Good Practice Guide is aimed at New Zealand Government Department ICT system administrators, ICT system installers and Departmental IT security managers.
6. This guide amalgamates GCSB subject matter expert knowledge and experience with KVM products in order to bring consistency to meeting the requirements of the New Zealand Information Security Manual (ISM) and manage risk effectively.
7. This guide **does not** replace the requirements of the ISM. It is essential that the ISM is reviewed in conjunction with this guide to ensure that requirements and any deviations from those are addressed.
8. Any queries relating to this guide and the implementation of the requirements within should be directed to GCSB.

## Key Words

9. Several words are used within this guide to signify the requirements of the ISM as determined by GCSB subject matter experts.
10. This language aligns with use within the ISM and is as defined by the International Engineering Task Force's (IETF's) request for comments (RFC) 2119 to indicate differing degrees of compliance. These key words can be found in **bold** so there is no doubt as to intention.

## UNCLASSIFIED

11. **MUST** This word, or the terms "**REQUIRED**" or "**SHALL**", mean that the definition is an absolute requirement of the specification. The specified item is mandatory.
12. **MUST NOT** This phrase, or the phrase "**SHALL NOT**", mean that the definition is an absolute prohibition of the specification. The specified item is mandatory.
13. **SHOULD** This word, or the adjective "**RECOMMENDED**", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. Where such an item is ignored, a risk management plan must be produced and followed.
14. **SHOULD NOT** This phrase, or the phrase "**NOT RECOMMENDED**" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label. Where such an item is ignored, a risk management plan must be produced and followed.
15. **MAY** This word, or the adjective "**OPTIONAL**", mean that an item is truly optional.

**Common Configuration**

16. The most common configuration is a desktop computer connected to the Internet and a second computer connected to a higher classification or private network each alternately operated from a single keyboard, single monitor and single mouse via a KVM as per figure 3.1. The process of connecting to a system simply involves selecting the desired network on the KVM via a switch or button.

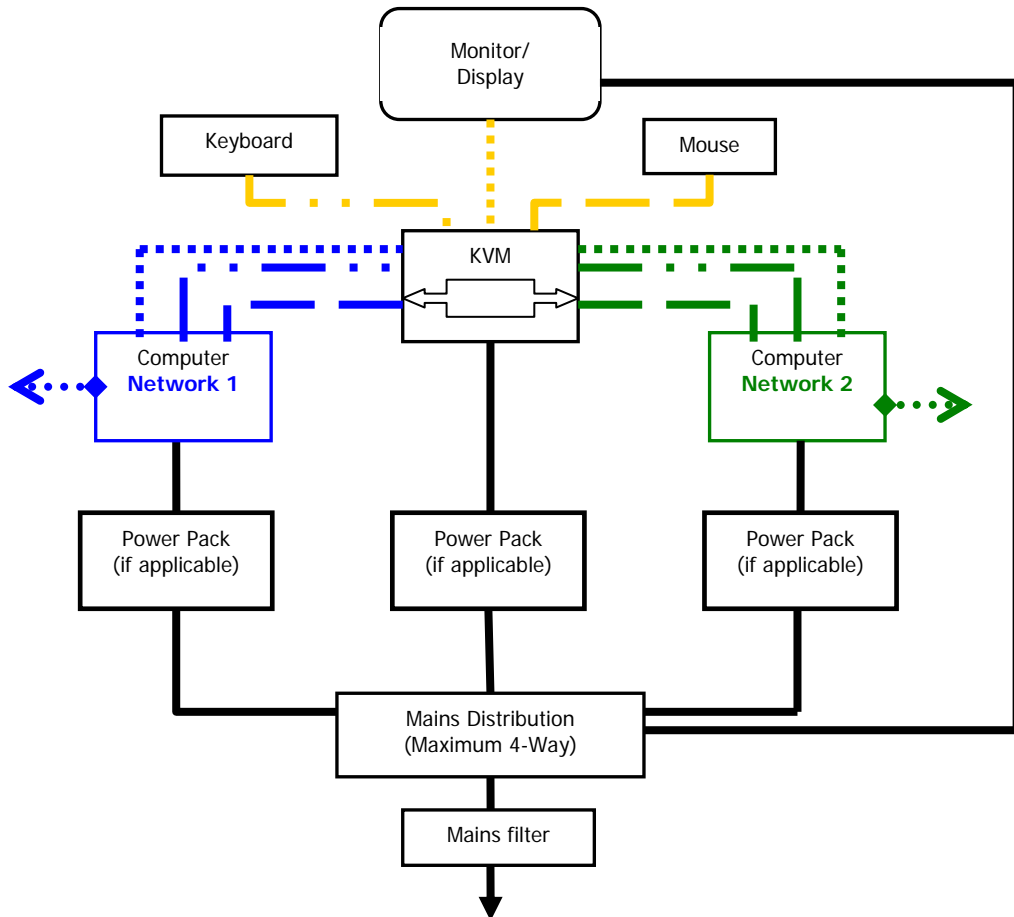


Figure 3.1 Common Configuration

# UNCLASSIFIED

## Principles

17. Properly installed and implemented KVM of appropriate assurance levels can prevent unintended interaction or operation occurring between or upon interconnected systems. In particular, preventing private or classified information being passed between networks.
18. The required level of assurance<sup>1</sup> of the KVM is determined by the highest and lowest classification of the networks to which it is connected.
19. High quality, professional installation of KVM switches and the associated network wiring is required, in particular to minimise TEMPEST risks associated with systems handling information of different classifications.
20. Proper software and hardware configuration, implementation and training are critical.

---

<sup>1</sup> The level of assurance (ISO 15408) is expressed as EAL-1 (lowest) to EAL-7 (highest) refer to the section titled Switching Requirements for further explanation.

# UNCLASSIFIED

## Risks

*The major risk with the use of a KVM is Operator Error where higher classified information may be inadvertently entered on a lower classified system.*

21. Principal risks associated with the use of KVM Switches include:

- a. Some models of KVM have the ability to share USB devices (such as printers), audio speakers and a microphone.
- b. Unintentional induced data “spill” from one network to the other. For example, by inadvertent selection of the lower classified network and subsequently entering classified information on that network;
- c. Compromising emanations (radiation of data) from the KVM, peripherals, and desktop wiring which may make data available for collection at some distance from the KVM switch and its wiring;
- d. Exfiltration of data from a private network or classified system by a third party when memory in a USB connected device (such as a printer) is covertly re-programmed from the Internet;
- e. Physical tampering of the KVM Switch to change its functionality so that classified information can be readily extracted;
- f. Malicious covert manipulation of KVM firmware or software programming while on one network to enable continuous illegal access of the other network;
- g. Poor installation practices, including failure to meet physical separation requirements between telephones and other devices;
- h. No logging, monitoring and/or follow up of inappropriate usage;
- i. Inadequate initial or follow-up training of users; and
- j. Best security practice is not followed by ICT system administrators, installers and users.

# UNCLASSIFIED

## Controls

22. It is impossible to fully mitigate the risk of third party electronic attack (eA) on the private network by covert manipulation of KVM programming other than by detaching it when not in use. The risk of eA is reduced when all controls and requirements within this guide are implemented.
23. To reduce the possibility of eA from one KVM connected network against the other, the KVM USB port **must** not be used to connect any device other than a keyboard and/or mouse. In particular, no devices with memory of any description are to be connected to the KVM USB port.
24. Information Assurance (IA) best practice is to connect a local computer to a network print server and avoid directly connecting desktop printers to the local computer.
25. To detect malicious physical access to the internal components of the KVM, tamper evident seals **should** be applied in such a manner to detect attempts at access.
26. A KVM **should** be considered with both:
  - i. An internal tamper switch disabling the KVM; and
  - ii. Employing locked memory to prevent reprogramming of firmware.
27. Any unused ports or connections on the KVM **should** be sealed so as to prevent and/or detect connection of unauthorised devices.
28. To reduce induced data “spill” from one network to another:
  - a. KVM products **must** be rated to the appropriate ISO-15408 level required for each application (refer the section titled Switching Requirements below);
  - b. Installation of equipment and wiring **should** be in accordance with New Zealand Communications Security Standard for Installation Engineering (NZCSS 400, available from GCSB);
  - c. Once installed movement of devices, wiring and/or network connections **should** be inhibited to as great an extent as possible and practicable;
  - d. Where a KVM is supplied with low voltage DC from a power supply, this supply **must** be used rather than relying on a USB power supply from either computer;
  - e. Mains filtering **should** be used on mains-powered devices, including the KVM power supply;
  - f. Where a mains distribution board is used, a maximum of a four-way mains distribution board is to be used. Any unused power sockets on the mains distribution board **should** be sealed so as to prevent connection of unauthorised devices;
  - g. All data connections **must** be through fibre optic cables to prevent classified emanations being coupled to unclassified networks. Copper connections such as STP and UTP are not to be used;
  - h. All fibre optic connections and fibre optic cables **should** be clearly labelled so as to be easily identifiable preventing incorrect interconnection of systems;

## UNCLASSIFIED

- i. Network fibre optic cables **should** be physically separated in order to prevent:
    - i. Inadvertent cross-connection of circuits of different classifications;
    - ii. Any optical cross-coupling of data;
  - j. A short fibre optic cable (with the appropriate driver units) **should** be used to isolate any Internet connected network from the final connection to the Internet. This will prevent propagation of any classified emanations that may have inadvertently coupled to the Internet connected network; and
  - k. The KVM Switch functionality that allows switching of loudspeakers and/or a microphone **must not** be used when any of the connected systems are classified CONFIDENTIAL or above.
29. To reduce radiation of data (emanations) from the KVM, peripherals and/or desktop wiring the controls above **should** be followed, plus:
- a. The native resolution<sup>2</sup> of the display device connected to the KVM **must** be used. Use of display devices at non-native resolution has been found to increase emanations;
  - b. Display adapters on each system **must** be tied to the native resolution of the display device;
  - c. The KVM to display device cable **should** be of the shortest possible length achievable;
  - d. Digital Video Interface Digital (DVI:D) **should** be used over Digital Video Interface I (DVI:I) which in turn **should** be used over Video Graphics Adaptor (VGA) for display device to KVM and KVM to computer video connections;
  - e. Where possible, the ability to reconfigure display resolutions by the user, **should** be disabled;
  - f. Suitably shielded cables **must** be used for all connections; and
  - g. Adaptors to convert plug or connector configurations **must not** be used.
30. Models of KVM may provide “on-screen” indication of the active network and/or use panel mounted indicator lighting. To identify to ICT system administrators and users which system is selected, prevent confusion between which system is in use and reduce inadvertent entry of classified data on the wrong system:
- a. Each system **must** provide an easily distinguishable background and banner;
  - b. The KVM **must** be clearly labelled to identify which system it is switched to and the classification of the corresponding system;
  - c. For a lower classified or Internet system interconnected by KVM to a CONFIDENTIAL or above system the user **should** lock the computer,

---

<sup>2</sup> The native resolution of a LCD or other flat panel display refers to its single fixed resolution. As an LCD display consists of a fixed raster, it cannot change resolution to match the signal being displayed such as a CRT monitor can, meaning that optimal display quality can be reached only when the signal input matches the native resolution. Most LCD monitors are able to inform the connected computer of their native resolution.

# UNCLASSIFIED

requiring user password to unlock the system, prior to switching between either system;

- d. TOP SECRET information requires more stringent controls due to the damage that unauthorised or unintentional release of this information would cause. Therefore, for an Internet system interconnected by KVM to a TOP SECRET system the user **must** log off the Internet system, requiring user name and password to log back onto the Internet system, prior to switching to the TOP SECRET system. Appropriate logging and monitoring **must** be employed; and
  - e. The user name and/or password **must** not be shared, i.e. the same, for interconnected systems of different classifications.
31. It is **recommended** that a robust content filtering system is employed on Internet systems interconnected by KVM to private or classified systems. GCSB is able to provide guidance on content filtering systems.
  32. Wireless peripherals **must not** be connected to the KVM or either computer.
  33. KVM power, the display device, keyboard and mouse **must** be the only connections to the KVM.
  34. Education of ICT system administrators and users of KVM is critical to protecting data and **should** be provided. Annex B provides best practice guidance for the use of KVM switches.
  35. Logging and monitoring of the KVM and interconnected systems **should** be employed to identify inappropriate usage. Any identified inappropriate usage **must** be investigated and managed accordingly.

### Switching requirements

36. For installations where KVM interconnected systems are classified RESTRICTED or below, an EAL2 rated KVM should be used.
37. For installations where one or more KVM interconnected systems are classified CONFIDENTIAL or above, the KVM should meet the level of assurance as indicated in the table below. In such circumstances departments **must** contact GCSB for further guidance and advice.

		System one					
		UNCLASSIFIED	IN CONFIDENCE	RESTRICTED or SENSITIVE	CONFIDENTIAL	SECRET	TOP SECRET
System two	UNCLASSIFIED	EAL-2					
	IN CONFIDENCE	EAL-2	EAL-2				
	RESTRICTED or SENSITIVE	EAL-2	EAL-2	EAL-2			
	CONFIDENTIAL	EAL-7	EAL-4	EAL-4	EAL-4		
	SECRET	HIGH GRADE	EAL-7	EAL-7	EAL-4	EAL-4	
	TOP SECRET	HIGH GRADE	HIGH GRADE	HIGH GRADE	HIGH GRADE	HIGH GRADE	EAL-4

**Matrix of KVM Assurance Levels**

38. Notes to Matrix of KVM Assurance Levels

## UNCLASSIFIED

- EAL rating is an ISO-15408 and Australian Information Security Evaluation Program (AISEP) rating. AISEP is a program under which evaluations are performed by impartial companies against the Common Criteria (CC). KVM products **must** be rated to at least the level listed.
  - High Grade refers to products that have been evaluated and appear on the Evaluated Products List (EPL).
  - For installations where the matrix requires use of EAL7, or HIGH GRADE rated KVM products departments **must** contact the GCSB for further information prior to installation and implementation of KVM.
39. Some UNCLASSIFIED networks **may** need to be highly protected; in such cases higher rated switches **should** be employed.
40. For a KVM used to connect a CONFIDENTIAL and above system with a system of lower classification, a KVM with physical switching between (button, switch etc) systems **must** be used.
41. A KVM which utilises either software switching or keyboard key-combination sequences **should not** be employed.
42. Where a KVM switch is used to switch between a Government network and the Internet the switch used **must** be rated at or above the appropriate ISO-15408 level of assurance for the classification of the Government network (refer the section titled Switching Requirements above).
43. Where a KVM switch is to be connected to switch between two networks of differing classifications the switch used **must** be rated at or above the appropriate assurance level of the higher classification.

### Installation requirements

44. The controls detailed above **should** be implemented as appropriate, additionally;
- i. Installation of the KVM switch and all of the network equipment, cables and wiring **must** be in accordance with the New Zealand Communications Security Standard for Installation Engineering (NZCSS 400, available from GCSB); and
  - ii. Physical separation requirements between systems of different classifications **must** be observed.

### Further Guidance

45. For further clarification Plain English KVM Installation Guidelines are available at Annex A.
46. GCSB is able to provide further advice and guidance on KVM related topics and specific requirements and applications.

**UNCLASSIFIED**

**Intentionally Blank**

**UNCLASSIFIED**

### Plain English KVM Installation Guidelines

#### Power Line Filtering

Power line filters must be used for each of the following groups of equipment:

- The PC and any ancillaries (such as a printer) connected to the higher classified network;
- The KVM and its ancillaries (such as the monitor and any speakers); and
- The PC and any ancillaries (such as a printer) connected to the lower classified network (e.g. the Internet).

Where a UPS is used, power line filters should be connected to the output side of the UPS and not the mains side.

If using a mains distribution board, a maximum of a four-way mains distribution board is to be used. Any unused power sockets on the mains distribution board must be sealed so as to prevent connection of unauthorised devices.

#### Use of Fibre Optics

All data connections to both the higher and lower classified networks must be through fibre optic cables to prevent classified emanations being coupled to unclassified networks. Copper connections such as STP and UTP are not to be used.

Label fibre optic connections and fibre optic cables so as to be easily identifiable preventing incorrect interconnection of systems.

#### Separation of Fibre Optic Cables

Fibre optic cables to the higher and lower classified networks should be physically separated in order to prevent:

- Inadvertent cross-connection of circuits of different classifications; and
- Any optical cross-coupling of data.

#### Optical Isolation

A short fibre optic cable (with the appropriate driver units) should be used to isolate any Internet connected network from the final connection to the Internet. This will prevent propagation of any classified emanations that may have inadvertently coupled to the Internet connected network.

#### Video Resolution

Use of display devices at non-native resolution has been found to increase emanations.

The resolution of any video display device (such as a LCD monitor) connected to the KVM should be set to the native resolution of the display device. Software switching of and user ability to modify the display device configuration should be disabled.

The native resolution of a LCD or other flat panel display refers to its single fixed resolution. As an LCD display consists of a fixed raster, it cannot change resolution to match the signal being displayed such as a CRT monitor can, meaning that optimal display quality can be reached only when the signal input matches the native

# UNCLASSIFIED

resolution. Most LCD monitors are able to inform the connected computer of their native resolution.

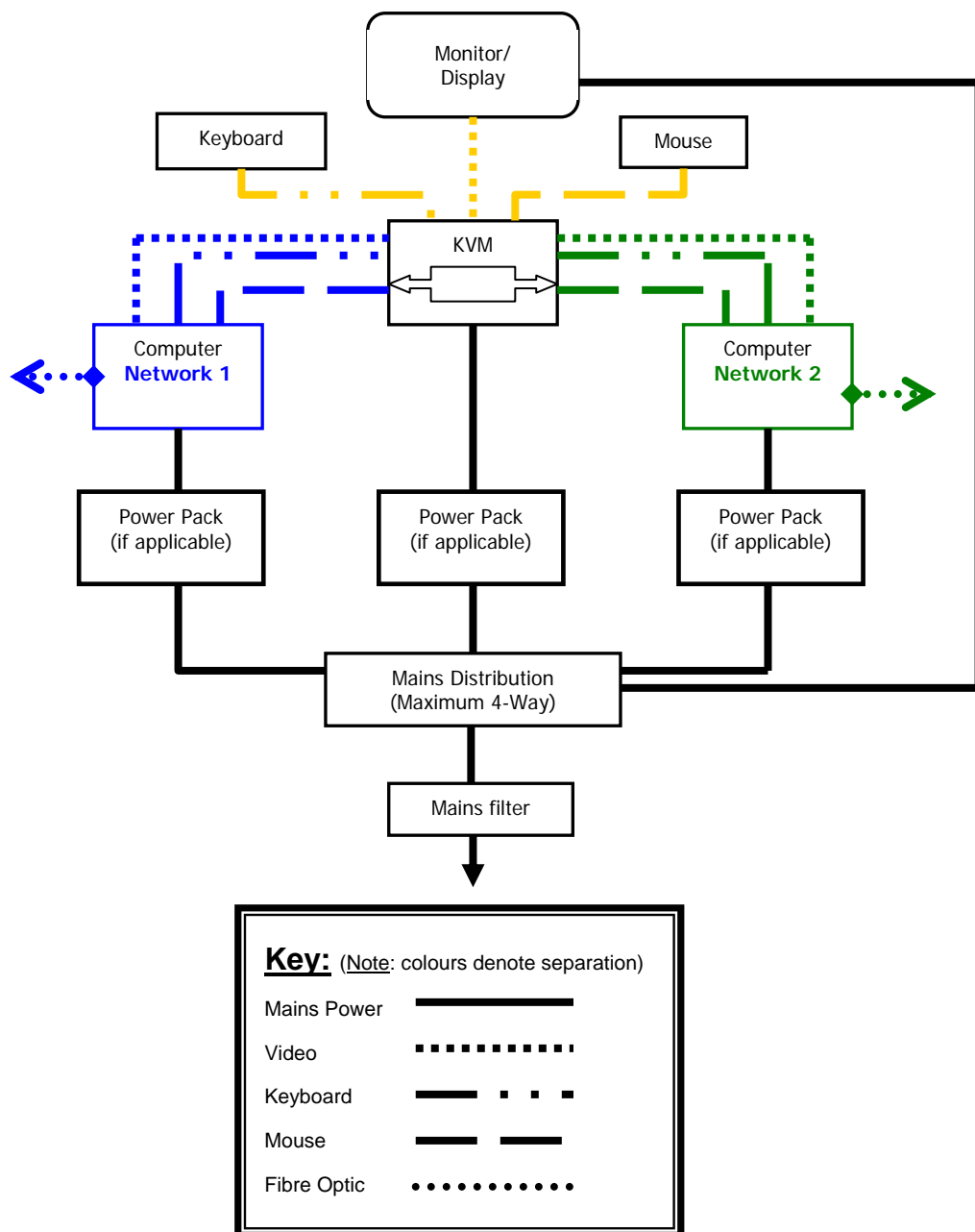
## Daisy Chaining

A KVM must not be “daisy chained” i.e. additional systems should not be connected via a second KVM plugged into the first. The KVM must have sufficient ports to allow connection of all required systems at each location.

## Adaptors

Adaptors to convert plug or connector types must not be used. Use cables with correct plug or connector configurations to directly connect between the KVM, computer and all other devices.

## Interconnectivity Diagram



### KVM User Best Practice Guidelines

#### Introduction

These guidelines are provided to ensure that ICT system administrators and users of systems with a KVM installed are aware of the security policies and responsibilities applicable to use of KVM.

#### Overview

A KVM is used to enable a single keyboard, display device (monitor) and mouse to be used with two separate computer systems which the KVM switches between as required by the user.

#### Installation

The installation of a KVM has been (or is to be) conducted by an authorised person in accordance with all applicable doctrine and policy.

Users are not authorised to connect or disconnect any device to the KVM or attached computer systems.

#### Tamper Proof Seals

The KVM is fitted with tamper proof seals that must be inspected prior to use.

Any evidence of tamper, such as broken or missing seals, must be reported to the departmental information security team, the KVM and interconnected computer systems must not be used until examined and cleared for use by the departmental information security team.

#### Component Separation

The components of each system, ancillary devices and phones must maintain specific separations from each other. Prior to moving KVM interconnected systems or any ancillary device/phone the departmental information security team or system installers must be consulted.

#### Audio and USB Devices

Audio and/or USB devices are not to be connected to a KVM, other than a USB keyboard or USB Mouse as installed by authorised installers.

#### Operation

Each KVM has subtle differences in operation and therefore users should seek appropriate training on the operation of the KVM and interconnected computer systems.

Users should be aware of:

- The method to switch between systems;
- Indications on the KVM as to which system is currently being accessed;
- Indications on the computer desktop displayed on screen as to which system is currently being accessed;
- Classifications of each system;

# UNCLASSIFIED

- Log on, Log off and screen lock policy for each system;
- What constitutes a security incident, action upon discovery and who to report incidents to; and
- Methods to lock/unlock and log off/on each system.

## **Logging and Monitoring**

Logging and monitoring of the KVM and interconnected systems must be employed to identify inappropriate usage. Any identified inappropriate usage must be investigated and managed accordingly.

**UNCLASSIFIED**

**Intentionally Blank**

**UNCLASSIFIED**

UNCLASSIFIED



**WARNING**

This document is the property of the New Zealand Government and contains official information protected by law. Unauthorised disclosure or use of the material contained herein is a criminal offence.

New Zealand Government

UNCLASSIFIED