12.6. Product Sanitisation and Disposal

Objective

12.6.1. All IT equipment is sanitised and disposed of in an approved and secure manner.

Context

Scope

12.6.2. This section covers information on sanitising and disposing of both evaluated and non-evaluated IT equipment. Additional information on the sanitisation, destruction and disposal of media can be found in Chapter 13 – Media and IT equipment management, decommissioning and disposal.

12.6.3. Media typically found installed in IT equipment are electrostatic memory devices such as laser printer cartridges and photocopier drums, non-volatile magnetic memory such as hard disks, non-volatile semi-conductor memory such as flash cards and volatile memory such as RAM cards. Some technologies, such as an FPGA, may integrate memory capabilities.

Rationale & Controls

Sanitisation or destruction of IT equipment

12.6.4.R.01. **Rationale**

In order to prevent the disclosure of classified information into the public domain agencies will need to ensure that IT equipment is either sanitised or destroyed before being declassified and authorised for released into the public domain. Refer also to Chapter 13 - Media and IT Equipment Management, Decommissioning and Disposal.

12.6.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3537]

Agencies MUST sanitise or destroy, then declassify, IT equipment containing **any** media before disposal.

12.6.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3540]

IT equipment and associated media that have processed or stored NZEO information, and cannot be sanitised, MUST be returned to New Zealand for sanitisation or destruction, declassification and disposal.

Disposal of IT equipment

12.6.5.R.01. **Rationale**

When disposing of IT equipment, agencies need to sanitise or destroy and subsequently declassify any media within the product that are capable of storing classified information. Once the media have been removed from the product it can be considered sanitised. Following subsequent approval for declassification from the owner of the information previously processed by the product, it can be disposed of by the agency.

12.6.5.R.02. **Rationale**

The GCSB provides specific advice on how to securely dispose of high assurance products, HACE and TEMPEST rated equipment. There are a number of security risks that can occur due to improper disposal, including providing an attacker with an opportunity to gain insight into government capabilities.

12.6.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3545]

Agencies MUST have a documented process for the disposal of IT equipment.

12.6.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3547]

Agencies MUST contact the GCSB and comply with any requirements for the disposal of high assurance products.

12.6.5.C.03.

Control System Classifications(s): All Classifications; Compliance: Must [CID:3549]

Agencies MUST contact the GCSB and comply with any requirements for the disposal of HACE.

12.6.5.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3550]

Agencies MUST contact GCSB and comply with any requirements for the disposal of TEMPEST rated IT equipment or if the equipment is non-functional.

12.6.5.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3552]

Agencies MUST formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain.

Sanitising printer cartridges and copier drums

12.6.6.R.01. **Rationale**

Electrostatic drums can retain an image of recently printed documents providing opportunity for unauthorised access to information. Some printer cartridges may have integrated drums. Printing random text with no blank areas on each colour printer cartridge or drum ensures that no residual information will be kept on the drum or cartridge.

12.6.6.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3555]

Agencies MUST print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

12.6.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3557]

Agencies SHOULD print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

Destroying printer cartridges and copier drums

12.6.7.R.01. **Rationale**

When printer cartridges with integrated copier drums or discrete drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them.

12.6.7.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:3561]

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, MUST destroy the cartridge or drum.

12.6.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3563]

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, SHOULD destroy the cartridge or drum.

Disposal of televisions and monitors

12.6.8.R.01. **Rationale**

Turning up the brightness to the maximum level on video screens will allow agencies to easily determine if information has been burnt in or persists upon the screen.

12.6.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3566]

Agencies MUST visually inspect video screens by turning up the brightness to the maximum level to determine if any classified information has been burnt into or persists on the screen, before redeployment or disposal.

Sanitising televisions and monitors

12.6.9.R.01. **Rationale**

All types of video screens are capable of retaining classified information on the screen if appropriate mitigation measures are not taken during the lifetime of the screen. CRT monitors and plasma screens can be affected by burn-in whilst LCD screens can be affected by image persistence which can led to LED/OLED burn-in.

12.6.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3572]

Agencies MUST attempt to sanitise video screens with minor burn-in or image persistence by displaying a solid white image on the screen for an

extended period of time. If burn-in cannot be corrected the screen MUST be processed through an approved destruction facility.

LCD/LED, plasma and non-CRT monitor types

12.6.10.R.01. **Rationale**

Current generations of monitors incorporate controllers to manage power up/power down, manage the display, operate any USB or other ports and manage the video data stream. The controller requires memory to operate and it incorporates some data storage capability and full write/read access to the display. It also retains settings and configuration. The underlying technology is often based on an FPGA and invariably requires some form of memory capability in order to operate.

Researchers have demonstrated that images can be recovered by directly accessing the controller and associated memory or analysing the orientation of the liquid crystals.

In addition monitors can be compromised to actively monitor or covertly steal data and even manipulate what is displayed on the screen. Other attacks exploiting monitors have also been demonstrated.

12.6.10.R.02. **Rationale**

Refer to Chapter 12 – Product Security and Chapter 13 – Media & IT Equipment Management, Decommissioning and Disposal for additional guidance.

12.6.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6997]

Because of the risks that data can be recovered from monitors, it is essential that any redeployment or disposal of monitors MUST follow the guidance in the NZISM.