11.8. Multifunction Devices, Network Printers and Fax Machines

Objective

11.8.1. Multifunction devices (MFD's), network printers and fax machines are used in a secure manner.

Context

Scope

11.8.2. This section covers information relating to MFDs, network printers and fax machines connected to either the ISDN, PSTN, HACE or other networks. Further information on MFDs communicating via network gateways can be found in Section 20.2 - Data Import and Export.

Rationale & Controls

MFD, network printer and fax machine usage policy

11.8.3.R.01. **Rationale**

MFDs, network printers and fax machines, are capable of communicating classified information, and are a potential source of information security incidents. It is therefore essential that agencies develop a policy governing their use.

11.8.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2537]

Agencies MUST develop a policy governing the use of MFDs, network printers and fax machines,

Sending fax messages

11.8.4.R.01. **Rationale**

Once a MFD or fax machine has been connected to cryptographic equipment and used to send a classified fax message it can pose risks if subsequently connected directly to unsecured telecommunications infrastructure or the public switched telephone network (PSTN). For example, if a fax machine fails to send a classified fax message the device will continue attempting to send the fax message even if it has been disconnected from the cryptographic device and connected directly to the public switched telephone network. In such cases the fax machine could then send the classified fax message in the clear causing an information security incident.

11.8.4.R.02. **Rationale**

Non-encrypted communications may be exposed in transmission and, if incorrectly addressed or an incorrect recipient number is entered, may cause a data breach.

11.8.4.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2543]

Agencies sending classified messages MUST ensure that the message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.

11.8.4.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2545]

Agencies MUST have separate MFDs or fax machines for sending classified messages and messages classified RESTRICTED and below.

Receiving fax messages

11.8.5.R.01. **Rationale**

Whilst the communications path between MFDs and fax machines may be appropriately protected, personnel need to remain cognisant of the need-to-know of the information that is being communicated. As such it is important that fax messages are collected from the receiving MFD or fax machine as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

11.8.5.C.01.

Control System Classifications(s): All Classifications; Compliance: Should [CID:2562]

The sender of a fax message SHOULD make arrangements for the receiver to:

- collect the fax message as soon as possible after it is received; and
- notify the sender immediately if the fax message does not arrive when expected.

Connecting MFDs to telephone networks

11.8.6.R.01. **Rationale**

When a MFD is connected to a computer network and a telephone network the device can act as a bridge between the networks. As such the telephone network needs to be accredited to the same classification as the computer network the MFD is connected to.

11.8.6.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must Not** [CID:2568]

Agencies MUST NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

11.8.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:2570]

Agencies SHOULD NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

Connecting MFDs to computer networks

11.8.7.R.01. **Rationale**

As network connected MFDs are considered to be devices that reside on a computer network they need to be able to process the same classification of information that the network is capable of processing.

11.8.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2575]

Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies MUST ensure that:

- each MFD applies user identification, authentication and audit functions for all classified information communicated by that device;
- these mechanisms are of similar strength to those specified for workstations on that network; and
- each gateway can identify and filter the classified information in accordance with the requirements for the export of data through a gateway.

Copying documents on MFDs

11.8.8.R.01. **Rationale**

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel need to be aware that if they scan or copy documents at a classification higher than that of the network the device is connected to they could be causing a data spill onto the connected network.

11.8.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:2578]

Agencies MUST NOT permit MFDs connected to computer networks to be used to scan or copy classified documents above the classification of the connected network.

Observing MFD and fax machine use

11.8.9.R.01. **Rationale**

Placing MFDs and fax machines in public areas can help reduce the likelihood of any suspicious use going unnoticed.

11.8.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2581]

Agencies SHOULD ensure that MFDs and fax machines are located in areas where their use can be observed.

Servicing and Maintenance

11.8.10.R.01. **Rationale**

Network and MFD printers invariably use hard disk drives, flash drives or other reusable storage which can contain copies of classified information. Any maintenance or servicing should be conducted under supervision or by cleared personnel.

11.8.10.R.02. **Rationale**

Copiers and laser printers may use electrostatic drums as part of the reproduction and printing process. These drums can retain a "memory" of recent documents which can be recovered. Any storage devices or drums replaced during maintenance should follow the prescribed media disposal and destruction processes (See Chapter 13 – Decommissioning and Disposal).

11.8.10.R.03. **Rationale**

Toner cartridges and other components may incorporate a memory chip, often used to track pages numbers and estimate print capacity. These chips have read/write capability and may pose a risk to classified systems. Once chips have been removed, the toner cartridges themselves may be disposed of through supplier recycling or other approved disposal channels.

11.8.10.C.01 **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:2589]

Any maintenance or servicing MUST be conducted under supervision or by cleared personnel.

11.8.10.C.02 **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:2590]

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.

11.8.10.C.03 **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:2591]

Toner cartridges MUST have the memory chip removed before the cartridge is recycled or otherwise disposed of. The memory chip MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.

11.8.10.C.04 **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2592]

Any maintenance or servicing SHOULD be conducted under supervision or by cleared personnel.

11.8.10.C.05 **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2593]

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing SHOULD be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.

USB Devices

11.8.11.R.01. **Rationale**

MFDs may also be equipped with USB ports for maintenance and software updates. It is possible to copy data from installed storage devices to USB devices. Any use of USB capabilities must be carefully managed.

11.8.11.C.01 **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2596]

The use of any USB capability MUST be conducted under supervision or by cleared personnel.

11.8.11.C-02 **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2597]

The use of any USB capability SHOULD be conducted under supervision or by cleared personnel.

Decommissioning and Disposal

11.8.12.R.01. **Rationale**

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.8.12.R.02. **Rationale**

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.8.12.C.01 **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2604]

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents MUST be disposed of following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.

11.8.12.C.02 **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2606]

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents SHOULD be disposed of

following the processes prescribed in Chapter 13 - Media and IT equipment Management, Decommissioning and Disposal.

Logging multifunction device use

11.8.13.R.01. **Rationale**

Centrally logging and analysing MFD events, which may include metadata and shadow copies of documents printed, scanned or copied by users, can assist in monitoring the security posture of systems, detecting malicious behaviour, and contributing to investigations following cyber security incidents. Logs are stored in a central system, such as a security information and event management tool or central database and can only be accessed or modified by authorised and authenticated users. Logs are stored for a duration informed by risk or regulatory guidelines.

11.8.13.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Should** [CID:7537]

Use of MFDs for printing, scanning, and copying purposes SHOULD be centrally logged.