

**STATE OF HAWAI'I
INFORMATION PRIVACY AND SECURITY COUNCIL**

Category	Security	Title	Multi-Function Copier/Printer Procurement Guidelines
Document:	IPSC2011-01	Revision:	2011.09.20
Posted URL:	http://ipsc.hawaii.gov		
Status:	Adopted	Revised on:	September 20, 2011
Authority:	State of Hawai'i IPSC	Exceptions:	Temporary Allowed
Applicability	<input checked="" type="checkbox"/> State Government Agencies <input checked="" type="checkbox"/> All Guideline <input type="checkbox"/> Excluding: None Not Applicable <input type="checkbox"/> Including: None Not Applicable <input checked="" type="checkbox"/> State Funded Entities Guideline <input checked="" type="checkbox"/> Other: County Government Agencies & Attached Guideline		

I. PURPOSE

The purpose of this document is to provide basic guidelines for all State and County agencies for protection of sensitive information on multi-function Copier/Printer (MFP) devices.

II. SCOPE

Directors and Chief Financial Officers will use these guidelines as a resource as they confer with their Technology Managers, to ensure that additional security features and functions of MFP devices meet or exceed government standards to protect and safeguard against unauthorized access to confidential and personal information.

Agencies/Departments that work with federal information of a confidential or personal nature must also ensure that MFP devices are in compliance with all federal requirements. These guidelines do not supersede agency specific guidelines established toward the authorization and access to confidential information.

III. BACKGROUND

Technology has increased the demand for more paperless operations, which has increased the need for scanning capability in many operational processes and communication protocols. Counties and State of Hawaii departments and agencies, must rely on MFP devices that will be appropriate to meeting increasing administrative needs.

IV. TERMS AND DEFINITIONS

Common Criteria - An international standard (ISO/IEC 15408) for computer security certification. Common Criteria (CC) is the abbreviated name for Common Criteria for Information Technology Security Evaluation. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

Cryptographic Boundary - An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module, and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic Module - The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and are contained within the cryptographic boundary.

Encryption - The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people. When utilizing encryption, the encryption solution must be a Federal Information Processing Standards (FIPS) 140-2 (as amended) minimum Level 1 certified cryptographic module.

Evaluation Assurance Level (EAL) – A numerical grade assigned following the completion of a Common Criteria security evaluation. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself, but rather the level the system was tested.

Multi-function Copier/Printer (MFP) devices – A device incorporating the functionality of multiple devices into one. Primarily performs the following functions: Print, Scan, Photocopy, Fax, and Email.

Personal Information (As defined in Act 135 and Act 136, Session Laws of Hawaii 2006) - An

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number;
2. Driver's license number or Hawaii identification card number; or
3. Account number: credit or debit card number, access code, or password that would permit access to an individual's financial account. (Note: Includes pCard/credit cards issued to employees for agency purchase purposes.)

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. HRS §487N-1

Sensitive Information – Any type of information such that the loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of the State of Hawaii. Examples of sensitive information include State of Hawaii infrastructure (physical and/or network) information and login accounts and passwords.

V. STANDARDS

A. HARD DRIVES

Encryption

Hard drive encryption will protect data at rest from unauthorized access. The following standards are required:

- If Personal or Sensitive Information is processed on the MFP, encryption must be utilized.
- The encryption solution must be a Federal Information Processing Standards (FIPS) 140-2 (as amended) minimum Level 1 certified cryptographic module. The recommended encryption to utilize is AES 128-bit.

Image Overwrite

Image overwrite is effective at removing data from the hard drive once the data is no longer needed. Image overwrite electronically "shreds" information on the hard drive(s) after a print, scan, fax or email. The following types of image overwrite must both be enabled:

- Immediate Image Overwrite – Automatically executed immediately after jobs are completed to remove image data from disk or other non-volatile storage.

And

- Scheduled Image Overwrite – Automatic, daily overwrite of all image data from disk or other non-volatile storage including any pending jobs (Department of Defense approved 3-pass algorithm).

Removal

If the MFP does not have disk encryption or immediate image overwrite, the hard drive must be removed and securely wiped or destroyed separately before it is disposed of or moved to a different agency.

If the MFP is leased, the vendor will remove the hard drive, securely wipe the hard drive of all data, and provide evidence (e.g., disk usage report) to verify that everything has been erased.

B. PRINTING

When printing documents containing Personal or Sensitive Information, immediately retrieve documents to avoid the disclosure of this type of information to unintended recipients.

If available, enable the secure printing option on the MFP. With secure printing, jobs are safely stored at the MFP until the owner enters a PIN to release them. This controls unauthorized viewing of documents sent to the printer.

C. NETWORK

Network Authentication and Authorization

Control access to print, scan, e-mail and fax features by validating user names and passwords prior to use of these functions. Authentication over the network must be done utilizing a secure protocol.

IP Filtering

Internet Protocol (IP) Filtering provides a means of restricting access to the system to a specific set or range of IP addresses. IP addresses outside of the allowed set or range are not permitted to access the MFP and any of its services. MFPs must be configured to allow only a set or range of IP addresses to access the MFP and any of its services.

Encryption with Secure Protocols

- If the MFP is connected to the network, encryption and secure protocols must be used to protect unauthorized access to data in transit. These protocols include: IPSec, SSL v3 /TLS (HTTPS), and SNMPv3
- If the Simple Network Management Protocol (SNMP) is used to manage the MFP, it must use SNMPv3. If SNMP is not needed, it should be disabled.
- Web-based administration must use SSL v3 / TLS or an equivalent protection (e.g., IPsec). Disable all insecure and unused management protocols (e.g., Telnet, File Transfer Protocol (FTP), SSL v1 and v2, and HTTP) and configure the remaining management protocols for least privilege.

Firewall

If the MFP is equipped with a firewall, it should be enabled. This will help manage communication between the MFP and authorized users.

Faxing

Unprotected fax connections in MFPs can be a “back door” into the network. Ensure that there is a complete separation of the fax telephone line and the network connection.

D. MFP ADMINISTRATION AND MANAGEMENT

Ensure that administrative functions and network settings cannot be viewed or changed, both locally and remotely, without a password.

Change the administrator password at install and on a regular basis for the MFP.

Subscribe to and regularly review vendor bulletins concerning security updates. Ensure that any security updates (e.g. Operating System, Firmware, Software, etc.) released by the vendor for the MFP are installed.

Thoroughly review vendor security configuration guides.

Develop a standard configuration and review regularly.

Enable audit logging on the MFP and review these logs periodically.

E. PROCUREMENT

Purchase a MFP device which has an EAL2 Common Criteria certification.

For MFPs not having the necessary security features, it is recommended to purchase the necessary security modules and enable the features.

For MFP security features that cannot be purchased or enabled, it is recommended to replace the MFP as soon as is appropriate. When the MFP is replaced, follow the hard drive removal standards found in this document.

VI. PERIODIC REVIEW

It is recommended that departments, agencies, and other jurisdictions, at its own discretion, conduct periodic reviews of their policy documents to ensure that employees are kept up to date with regards to new and additional policy requirements and to restate existing policy requirements. These periodic

reviews shall remind users of their responsibility in the proper use of the department's information technology resources and their obligation in protecting confidential agency resources, information, and data. Users shall be required to resign the acknowledgement document once the periodic review has been completed.

VII. REFERENCES

Hewlett-Packard Development Company, L.P., HP Imaging and Printing Security Best Practices

<http://www.esi.net> Retrieved July 2010 from the World Wide Web:

<http://www.esi.net/Images/Interior/factsheet.pdf>

<http://www.xerox.com>. Retrieved July 2010 from the World Wide Web:

<http://www.xerox.com/information-security/product-security/enus.html>

United States Department of Commerce, National Institute of Standards and Technology, Glossary of Key Information Security Terms (NIST IR 7298)

Xerox Multifunction System Security Presentation, May 20, 2010:

<https://www.brainshark.com/xerox/MultifunctionSystemSec052010>

VIII. COMMENTS AND SUGGESTIONS

Comments, recommendations, proposals, or suggestions regarding the contents of this document may be sent via email to:

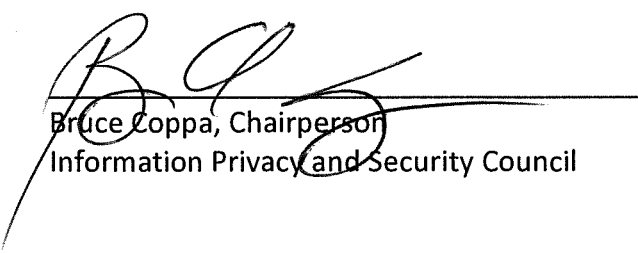
IPSC@hawaii.gov

or in writing to:

Information Privacy and Security Council
c/o Information and Communication Services Division
1151 Punchbowl Street, Room B10
Honolulu, HI 96813

IX. REVISION HISTORY

Creation Date: January 19, 2011	Date Last Updated September 20, 2011	Date last reviewed September 20, 2011
Revision History		
Revision date	Revision	Author
09/20/2011	First Issue	IPSC


 Bruce Coppa, Chairperson
 Information Privacy and Security Council

9/21/11
 Date