



DEPARTMENT OF THE ARMY
JOINT BASE MYER – HENDERSON HALL
204 LEE AVENUE
FORT MYER, VIRGINIA 22211-1199

REPLY TO
ATTENTION OF

IMMH-AO

SEP 16 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Joint Base Myer-Henderson Hall (JBM-HH) Policy Memorandum AO-3, Joint Base Commander's Information Protection (SecurePrint) and Printer Policy

1. REFERENCES.

- a. Army Regulations 25-1, Army Information Technology, 25 Jun13.
- b. Army Regulation 25-2, Information Assurance, Rapid Action Revision, 23 Mar 09.
- c. National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personal Identifiable Information (PII), 29 Feb 12.

2. PURPOSE. Provide guidance to all JBM-HH personnel on the Joint Base Information Protection (SecurePrint) and Printer Use Policy.

3. APPLICABILITY. This policy is applicable to all military, civilians, contractors and volunteers who handle PII and are assigned to and/or under the operational control of the JBM-HH.

4. POLICY.

a. Protecting sensitive information is the personal responsibility of every military, civilian, contractor, and volunteer who handles PII in the performance of their duties. In an effort to improve the safeguarding and handling of sensitive information, SecurePrint technology has been purchased by this command. This policy provides direction on the use of this technology.

b. For the purpose of this policy, the term "Sensitive Information" includes, but is not limited to the following types of information:

- (1) Name, such as full name, maiden name, mother's maiden name, or alias.
- (2) Personal identification number, such as social security number, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number.
- (3) Address information, such as street address or personal email address.
- (4) Asset information, such as Internet Protocol or Media Access Control address or other host-specific persistent static identifier that consistently links to a particular person or small well-defined group of people.

IMMH-AO

SUBJECT: Joint Base Myer-Henderson Hall (JBM-HH) Policy Memorandum AO-3, Joint Base Commander's Information Protection (SecurePrint) and Printer Policy

(5) Personal telephone numbers, including home and mobile.

(6) Personal characteristics, including photographic image (especially of face or other distinguishing characteristics), x-rays, fingerprints, or other biometric image or template data (retina scan, voice signature, facial geometry).

(7) Information identifying personally-owned property, such as vehicle registration number or title number and related information.

(8) Information about an individual that is linked or linkable to one of the above (date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, financial information).

c. Users printing documents containing sensitive information will use the SecurePrint feature to ensure information confidentiality. Instructions for using this feature are attached to this policy memorandum. Additional copies may be requested from the Information Management Officer.

d. When using the CAC Scan feature to scan documents containing sensitive information, users will use the encryption option to ensure data confidentiality.

e. Additionally, the purchase of, supplies for, and maintenance of personal stand-alone printers is prohibited. Exceptions to this policy may be granted by the JBM-HH Commander or Chief of Staff on a case-by-case basis. Those with stand-alone printers may continue to use them until the current stock of supplies has been exhausted or the device becomes non-functional. Once current supplies are exhausted, stand-alone printers will be turned in to the Property Book Office for official disposition and removal from the organization's property book. The Government Purchase Card shall not be used to purchase any printing supplies except paper.

5. PROCEDURES. A copy of this memorandum will be posted on unit and directorate bulletin boards where all unit/directorate members will have access to it.

6. PROPONENT. The JBM-HH S-6 Office is the proponent for this policy. The point-of-contact is the Information Management Officer at commercial (703) 696-0481 or DSN 426-0481.

DUGGAN.PATRICK
.MICHAEL.1068312
120

Digitally signed by
DUGGAN.PATRICK.MICHAEL.1068312120
DN: c=US, ou=U.S. Government, ou=DoD,
ou=PKI, ou=USA,
cn=DUGGAN.PATRICK.MICHAEL.1068312120
Date: 2016.09.15 15:46:05 -0400

PATRICK M. DUGGAN
COL, SF
Commanding

DISTRIBUTION: 1

Using SecurePrint on the Ricoh MFD's

Install the Driver

Click Start → Type [\\160.145.40.44](http://160.145.40.44) in the search box and press enter (Or click the link) → Double Click the SecurePrint icon and wait for the driver to install itself. This may take a few minutes. Once installed, open Printers and Devices from the Start Menu and look for this icon in your Printers and Faxes area:



Using SecurePrint

To use SecurePrint, simply select "SecurePrint on 160.145.40.44" as your desired printer when printing. Then, go to any Ricoh MFD and select the "SecurePrintScan" button from the Home screen. Insert your CAC into the CAC reader and enter your pin when prompted. Select OK and wait for authentication to complete. You will then be presented two options, "Release My Print" or "Scan to My Email". Select "Release My Print" and your print jobs will be displayed. Select the job you wish to print and click "Print".

General Information and Guidance

SecurePrint technology is designed to allow you to print sensitive documents to shared network printers without the risk of information compromise. A feature of this technology is "Follow Me Printing", which allows you to go to any Ricoh MFD and print your documents. So, if you want color prints of something, you simply go to a color MFD and release your print job. The print jobs will stay in the print cue for 72 hours before the system will delete them. Once printed, you will still have access to those print jobs for 7 days.

A formal policy signed by the Commander will be released in the coming weeks that will direct SecurePrint to be used for all print jobs containing Personally Identifiable Information (PII), evaluations, financial information, addresses, alert rosters, etc. The intent is to reduce the chances of accidentally releasing or exposing sensitive information to those without a valid need to know.

Additionally, the new Ricoh MFD's are capable of encrypting scans, so if you are scanning documents like those listed above, you must encrypt them.