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

AMIM-MHO

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Joint Base Myer-Henderson Hall (JBM-HH) Policy Memorandum PL-5, Operations Security (OPSEC)

1. REFERENCE. AR 530-1, Operations Security (OPSEC), 26 Sep 14.

2. PURPOSE. To provide guidance to all JBM-HH personnel on incorporation of OPSEC practices and procedures into daily activities.

3. APPLICABILITY. This policy applies to all Department of the Army (DA) personnel, military and civilian, working in the JBM-HH community.

4. POLICY. OPSEC is the security of plans, operations and activities. OPSEC denies access to critical information by identifying, controlling, and protecting indicators and information sources associated with the planning and execution of actions, as well as the existence and capabilities of an activity. OPSEC practices and procedures will be integrated into day-to-day operations at all JBM-HH activities. It is a security process that must be taken as seriously as the protection of classified information.

5. PROCEDURES.

a. All Army and Marine products containing sensitive but unclassified information (Critical Information, For Official Use Only (FOUO), Privacy Act Information, etc.) should be destroyed as classified trash. Shredding is the principal method for destruction using GSA-approved shredders. All other information developed as part of the job should be disposed of appropriately.

b. “For Official Use Only” will be the standard marking for all unclassified products determined to be Critical Information by each directorate in coordination with the OPSEC Program Manager. Critical Information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and information needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.

c. All classified e-mail must be sent via classified computer network Secret Internet Protocol Router Network (SIPRNET).

d. All unclassified official e-mail going outside of JBM-HH to higher headquarters will be sent encrypted and have the proper classified markings at the beginning and end of the message (e.g., Unclassified FOUO). All official e-mail sent within JBM-HH containing privacy act information will also be sent encrypted.

e. Classified telephone conversations will be made on a secure telephone (STU/STE/SVOIP).

f. Every effort should be made to keep work areas clear of classified documents, sensitive information and privacy information, including telephone numbers. Offices should use the Standard Form 701 to ensure work areas are OPSEC clean. The last individual leaving the office or work area is responsible for ensuring the area is cleared of classified, official use only documents, and privacy information. In addition, before individuals take extended leave or go TDY, they should clean their area of all documents containing classified, sensitive or critical information.

g. All JBM-HH personnel will consult with their immediate supervisor and/or the Directorate OPSEC Coordinator prior to publishing or posting information in any public forum to ensure no Critical Information or indicators are released. This includes but is not limited to letters, email, websites, web logs and information forums. Supervisors will review documents to ensure Critical Information and indicators of Critical Information are not released. Each unit or agency OPSEC Coordinator should advise their supervisors on means to prevent the release of Critical Information.

h. Each Director is responsible for appointing a representative to attend the Protection Working Group this should be their OPSEC Coordinator. Directors will also annually review the Installation Critical Information List and develop an installation acceptable OPSEC risk for the Commander.

i. Information Assurance (IA) is a crucial element of the OPSEC process. IA establishes policies and assigns responsibilities for all users and developers for achieving acceptable levels of IA in the engineering, implementation, operations, and maintenance for all information systems, including telephones, facsimile machines, computer networks, and modems. All government equipment is subject to monitoring for telecommunications security purposes at all times. All users will report security incidents to the Information Assurance Program Manager, Network Enterprise Center Fort Myer.

j. Annual training for OPSEC and Information Assurance is mandatory. OPSEC Level 1 (Newcomers and refresher) training is web based training (WBT) found @ https://securityawareness.usalearning.gov/opsec/index.htm. Information Assurance training is also WBT accessible at https://atc.us.army.mil/iastar/index.php..

6. PROPONENT. The Directorate of Plans, Training, Mobilization and Security is the proponent for this policy. POC is the OPSEC Program Manager, 703-696-0756.

BOWLING.DAVID.DARRELL.1135102829

Digitally signed by BOWLING.DAVID.DARRELL.1135102829
Date: 2021.06.03 10:23:33 -04'00'

DAVID D. BOWLING
COL, SF
Commanding

DISTRIBUTION:
I