DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM, NEW YORK 13602-5000

AFDR-CG 12 July 2021

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Policy Memorandum 21-13, Personally Identifiable Information (PII)

1. References:

a. Army Regulation (AR) 25-22, The Army Privacy Program, 22 December 2016.

b. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

c. DoD OSD Memorandum, Subject: Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations, 2 August 2012.

d. DoD OSD Memorandum, Subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 21 September 2007.

e. DoD Directive 5400.11, Department of Defense Privacy Program, 29 October 2014.

f. OMB Memorandum, M07-16, Subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 22 May 2007.

2. Supersession: This policy supersedes and replaces Installation Policy Memorandum 19-13, Personally Identifiable Information (PII), 17 September 2019.

3. Purpose: Explains PII and includes specific procedures on protecting and reporting PII incidents.

4. Applicability: This policy applies to all organizations/units/activities and their personnel (Soldiers, Civilians, and contractors) who receive computer service from the Fort Drum Network Enterprise Center, and/or conduct business on Fort Drum.

5. General:

a. All personnel are required to protect PII (in physical or electronic form) from unauthorized use, access, disclosure, alteration, or destruction.

b. Personally identifiable information is information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life. Information includes but is not limited to education, financial transactions, medical history, criminal or employment history, and other which can be used to distinguish or trace an individual's identity (i.e., name, social security number, date and place of birth, mother's maiden name, biometric records, etc.). Personnel are to limit the amount of PII collected and stored on computer systems and mobile communication.

c. A breach is defined as an actual or possible loss of control, unauthorized disclosure, or unauthorized access to PII.

d. All personnel must be knowledgeable of the procedures for protecting PII (Encl 1) and reporting the breach or loss of PII (Encl 2).

e. An incident is when PII is suspected or confirmed to be lost, stolen, or otherwise available to individuals without a duty-related official need to know. This includes posting PII on a public website, sending PII to unauthorized recipients, providing hard copies of PII to individuals without a need to know, and losing electronic devices storing PII.

f. Failure to protect PII may result in punitive action.

6. The points of contact for this policy are the Administrative Services Division Chief at (315) 772-5288 and the Information System Security Manager at (315) 772-4412.

2 Encls
as

MILFORD H. BEAGLE, JR.
Major General, USA
Commanding

DISTRIBUTION: A