AFRC-CI

15 November 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Electronic Mail Use, Digital Signature, and Encryption Policy

1. References:
   c. JTF-GNO CTO 07-015 Public Key Infrastructure (PKI) Implementation, Phase 2, Revision 1, 7 April 2008.

2. Purpose: This policy defines the acceptable use of United States Army Reserve (USAR) electronic mail (email) resources and outlines the proper use of email, digital signatures, and encryption.

3. Applicability: This policy applies to all personnel using email and resources on USAR managed networks (unclassified and classified).

4. Policy:
   a. USAR personnel are prohibited from using:
      (1) Commercially provided email services for any official Government business and communication. Personnel will only use Government provided email services such as Enterprise Email for official communications.
      (2) Automatic forwarding from an official Government account to an unofficial (commercial service) account. Personnel may automatically forward messages from one official Government account to another Government account owned by the same user and at the same classification level.
      (3) Government email accounts for personal business affiliations. Use caution when using Government email addresses for commercial, affiliated organizations, or online retailers; users should only provide these email addresses to recognized and
AFRC-CI
SUBJECT: Electronic Mail Use, Digital Signature, and Encryption Policy

trusted entities. Commercial associations increase the potential for abuse, spam, marketing, account resale, and other social engineering attacks.

b. Digital signatures are required on all Government emails that contain an embedded hyperlink and/or attachment. Automated email notifications, such as a help desk mailbox that automatically sends standard responses to user inquiries, do not require a digital signature. Pure text references to web addresses, URLs, or email addresses do not require a digital signature; this requirement only pertains to active content and/or attachments.

c. Personnel must encrypt and digitally sign email containing personally identifiable information (PII) or sensitive information.

d. General Officers and Senior Executive Service personnel must digitally sign and encrypt all Nonclassified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) email when communicating with other senior level officials through the use of a Common Access Card (CAC) or equivalent hardware token in accordance with AR 25-2, section VII, paragraph 4-20.

5. Effective Date: This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.

6. The point of contact for this policy is Mrs. Kimberly Register, Chief, USARC CIO/G-6 Cybersecurity Program Management Division, (910) 570-8653 or kimberly.m.register.civ@mail.mil.

DENIS L. GIZINSKI
Chief Information Officer
Deputy Chief of Staff, CIO/G-6

DISTRIBUTION:

GEOGRAPHIC COMMANDS:
1 MSC
7 MSC
9 MSC
(CONT)
AFRC-CI
SUBJECT: Electronic Mail Use, Digital Signature, and Encryption Policy

DISTRIBUTION: (CONT)
63 DIV (R)
   - USAG-FHL
81 DIV (R)
   - USAG-Fort Buchanan
88 DIV (R)
   - USAG-Fort McCoy
99 DIV (R)
   - ASA-Dix

FUNCTIONAL COMMANDS:
3 MCDS
76 ORC
79 TSC
200 MP CMD
311 SC(T)
335 SC(T)
377 TSC
412 TEC
416 TEC
807 MCDS
ARAC
ARCD
AR-MEDCOM
LEGAL CMD
MIRC
USACAPOC(A)
75 TNG CMD (MC)
80 TNG CMD (TASS)
83 US ARRTC
84 TNG CMD (UR)
85 USAR SPT CMD
108 TNG CMD (IET)
USAR SPT CMD (1A)

AREC/ARET:
USARPAC
ARNORTH
AR SOUTH
ARCENT
(CONT)
AFRC-CI
SUBJECT: Electronic Mail Use, Digital Signature, and Encryption Policy

DISTRIBUTION: (CONT)
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

COPY FURNISH:
USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies