DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CI

15 November 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Password Policy for System/Service Accounts

1. References:

a. Army Regulation (AR) 25-2, Rapid Action Revision, Information Assurance, 23 March 2009.

b. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (updated 22 January 2015).

2. Purpose: This policy outlines the requirements for passwords generated by the United States Army Reserve Command (USARC) Chief Information Officer (CIO)/G-6 Data Systems and Applications Branch for approved system/service accounts for all USAR managed networks (unclassified or classified).

3. Applicability: This policy applies to all system/service accounts for information systems on United States Army Reserve (USAR) managed networks.

4. Policy: All passwords must meet the history, age, length, and complexity requirements in accordance with reference 1b. USARC CIO/G-6 Data Systems and Applications Branch will reissue a new password for all group/shared accounts as soon as an administrative user leaves the organization.

a. History: Do not re-use one of the last 24 passwords used previously for the account.

b. Frequency:

(1) Change passwords no later than 60 days after account creation.

(2) Do not change passwords for an account more than once every 24 hours.

(3) Change group account passwords when a System/Network Administrator who knows the password leaves the organization.

c. Minimum Length: Passwords will contain at least 15 characters.

d. Complexity: All system/service account passwords will include at least one uppercase letter, one lowercase letter, one number, and one symbol.

e. All Application Owners, System Owners, and System/Network Administrators responsible for creating, enforcing, and validating passwords will comply with this policy, AR 25-2, and other applicable regulations.

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 Effective Date: This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.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 memorandum 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, G-6

DISTRIBUTION:

GEOGRAPHIC COMMANDS:
1 MSC
7 MSC
9 MSC
63 DIV (R)
- USAG-FHL
81 DIV (R)
- USAG-Fort Buchanan
88 DIV (R)
- USAG-Fort McCoy
99 DIV (R)
- ASA-Dix
(CONT)

DISTRIBUTION: (CONT)

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
ARSOUTH
ARCENT
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
(CONT)

DISTRIBUTION: (CONT)
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

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