


INDIAN AFFAIRS DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER 65 IAM 2	SUBJECT Network Account Password Policy	RELEASE NUMBER 07-43
FOR FURTHER INFORMATION Office of Chief Information Officer		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

This document establishes Indian Affairs (IA) policy for the implementation and maintenance of network account passwords. Execution of this policy increases the security of the network and reduces the potential for intrusion into IA information systems. Employee compliance is mandated to protect both the agency and the employee.



Debbie L. Clark
Deputy Assistant Secretary – Indian Affairs (Management)

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 2

1.1 Purpose. This document establishes Indian Affairs (IA) policy for the implementation and maintenance of network account passwords. Execution of this policy increases the security of the network and reduces the potential for intrusion into Bureau of Indian Affairs (BIA) information systems. Employee compliance is mandated to protect both the agency and the employee.

1.2 Scope. This policy applies to IA employees, contractors, and non-IA staff accessing BIA information technology systems and equipment.

1.3 Policy.

A. General

- a. All accounts on the system shall maintain a strong password.
- b. The Division of Information Security and Privacy (DISP) shall validate the use of strong passwords on a quarterly basis and warn the user to change his/her password if it is not in compliance with the password-complexity requirements to protect the security of BIA networks.
- c. All default user passwords shall be changed upon initial access by the user to BIA systems.
- d. All default system passwords shall be changed from factory installed settings.
- e. Passwords shall be between eight and fourteen characters in length.
- f. Passwords shall consist of characters from at least three of the following four classes:
 - i. Upper case letters such as A, B, and C
 - ii. Lower case letters such as a, b, and c
 - iii. Numerals such as 0, 1, and 2
 - iv. Special characters such as !, @, #, \$, %, ?, +.
- g. The password shall be subjected to a periodic dictionary-check to identify weaknesses.
- h. The password setting for all BIA information systems shall be configured to expire in 90 days.
- i. Passwords can only be changed once in a 24-hour period unless the user suspects that a password has been compromised. In that case, the user shall change it immediately and notify the IA Help Desk.
- j. Passwords to special privileged accounts such as Administrator for sensitive-information resources attached to the BIA network shall be documented in a secure location such as a safe, and will be accessible only in emergencies by the Bureau Information Technology Security Manager (BITSM) or Chief Information Officer (CIO).
- k. User accounts shall be set to lock-out access for at least 60 minutes after five unsuccessful logon attempts.
 - i. The system security policy settings enforce logging of successful and failed logon attempts.
- l. A user shall contact the IA Help Desk when the user forgets his/her password or has been locked-out of the system due to failed log-on attempt.

- i. After verifying the identity of the user, the Help Desk shall reissue or unlock the user account.
- m. Authorized users shall be responsible for maintaining the security and privacy of their credentials.
 - i. Passwords shall not be written down or stored in clear text on systems or other devices such as Personal Digital Assistants (PDAs).
 - ii. Passwords shall not be disclosed to anyone for any reason.

B. Prohibitions

- a. Users shall not run password-cracking programs or password sniffers on BIA systems.
- b. Passwords shall not be displayed in clear text when entering in any BIA systems.
- c. The password shall not include characters that form a sequential set of keys on the keyboard such as asdf, qazwsx, 1234.
- d. Passwords shall not be reused during the next 10 password change selections.
- e. Passwords shall not contain any form of the user's first or last name or user ID.

1.4 Authority.

A. Department of the Interior (DOI) Computer Security Handbook V1.0

B. Federal Financial Management Improvement Act of 1996 (FFMIA)

C. Federal Information Processing Standards (FIPS)

- a. 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003
- b. 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- c. 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006

D. Federal Information Security Management Act of 2002 (FISMA)

E. National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems

F. Office of Management and Budget (OMB)

- a. **Circular A-130, Management of Federal Information Resources**, Appendix III, Security of Federal Information Resources, November 2000
- b. Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 2003

1.5 Responsibilities.

A. Chief Information Officer and OCIO Staff are responsible for creating and/or revising information technology policies and ensuring that the information in the IAM for the programs and functions within their authority, including references and citations, is accurate and up-to-date.

B. Bureau Information Technology Security Manager (BITSM) shall ensure that the policy and processes in the IAM conform to applicable statutes, regulations, Federal standards, and policies.

C. Authorized IA Users, defined as IA employees, contractors, and other individuals who have been granted explicit authorization to access, modify, delete, or utilize IA information, shall adhere to this policy.

1.6 Sanction of Misuse. In accordance with 370 DM 752, personnel are individually responsible for protecting the confidentiality, availability, and integrity of data and information accessed, stored, processed, and transmitted. Individuals are accountable for actions taken on and with IA and BIA IT information resources. Failure to comply with this policy may lead to disciplinary action. Unauthorized disclosure of sensitive information may result in criminal or civil penalties.