

PURPOSE:

This policy implements NIST, DHHS and NIH password policies for eRA/ORIS information systems environments, and includes both password and lock-out requirements. It meets the requirements of NIH password policies, which are documented in memoranda titled NIH Password Policy revised, January 2008.

NOTE: This document supersedes the previous IMPAC II Password Policy dated June 2007.

BACKGROUND/HISTORY:

It is imperative that users practice due diligence in controlling access to their system by protecting their user accounts with passwords which are not easily guessed or deduced.

PERSONS AFFECTED:

This policy is applicable to all federal employees, contractors and external users of eRA/ORIS information systems and technologies.

POLICY:

This policy is intended to reduce the risk of unauthorized access to eRA Applications and databases essential to the mission of the eRA program. The following principles apply:

- **Complexity:** Passwords must be at least eight (8) non-blank characters in length and contain three of the following types of characters: capital letters, lower case letters, numeric characters and at least one of the following special characters ! # \$ % - _ = + < >
- **Frequency of change:** Passwords must be changed at least once every 60 days, and cannot be the same as the past 24 passwords for the same user.
- **Caching:** Saving passwords to the system, and using automatic logins is prohibited. Storing passwords in files on the user's system is also prohibited.
- **Sharing Passwords:** Providing your password to someone else to use, or utilizing another user's password is prohibited.
- **Lock-out:** Systems will lock-out a user account after 6 failed attempts within 30 minutes to login with a wrong password. Account lock-out duration is 1 hour or until reset by an authorized administrator.
- **System Inactivity:** When users will be away from their systems for more than 30 minutes, the systems must be either locked or logged off.

-
- **Encryption:** The transmission of all passwords from both inside and outside the eRA security perimeter will be conducted using NIST-approved encryption.
 - **Account Inactivity:** If the accounts are inactive for more than 180 days, the account is automatically locked, and the IC Technical Coordinator (following appropriate rules) must re-issue the role through the User Admin module.

ENFORCEMENT:

eRA/ORIS Management has approved this policy; compliance and enforcement will be under the direction of the ISSO.

NEED ASSISTANCE?

For further assistance with password issues, please contact the eRA Helpdesk.

- Online Service Request: <http://itservicedesk.nih.gov/eRA/>
- E-mail address: helpdesk@od.nih.gov
- Phone number: 301-402-7469

ISSUE DATE AND REVISION HISTORY:

Issued: July 2003

Revision: June 2007

Revision: May 2008