Electronic Research Administration Procedure

Policy
eRA Pxxx

National Institutes of Health

Approved: TBD

SUBJECT: Password Policy for Publicly Available eRA Applications

(Latest Revision: March 2009)

Purpose and Scope

This policy ensures the confidentiality, integrity, and availability of publicly available eRA applications by protecting user accounts with strong passwords that meet the criteria of NIST, HHS, and NIH.

Applicability

This policy applies to users who access publicly available eRA applications.

Policy

- **Password Complexity:**
  - Passwords must be at least eight (8) non-blank characters in length
  - Passwords must contain a combination of at least three of the following types of characters:
    - capital letters
    - lower case letters
    - numeric characters
    - special characters
      ! # $ % - _ = + < >*
  - Passwords cannot contain username
  - First and last characters cannot be numbers

- **Changing Passwords:** Passwords must be changed at least every 90 days and the password cannot be reused within one year. Users must change their newly assigned passwords the first time they log on.

- **Account Lock-out:** Systems will lockout a user account after 6 consecutive failed login attempts.

- **User Session Inactivity:** System will disconnect user sessions that are idle longer than 45 minutes.

- **Caching Passwords:** Users are prohibited from caching (auto-saving) passwords on the local system. Users must enter the password at each login. Storing passwords in files on the user's system is prohibited.

- **Sharing Passwords:** Users are prohibited from sharing passwords with each other and each user must have a separate and unique password. Users should not allow others to access resources under their credentials by logging on and then letting others use the computer.

- **Password Distribution and Storage**: Passwords must be stored, transmitted, and distributed in a secure manner. Passwords must not be displayed on the screen when entered. Electronically storing or transmitting passwords in plain text is prohibited.

- **Audit:** Accounts and their adherence to the password policy will be audited periodically.

- **Compromised Passwords:** Compromised passwords must be reported to the eRA Help Desk. Please see contact information below.

References

NIH Password policy dated Oct. 5, 2004 (Revised Feb. 26, 2008) and located at: http://irm.cit.nih.gov/nihsecurity/pwd_policy.doc

.

Enforcement

eRA Management has approved this policy; compliance and enforcement will be under the direction of the Information System Security Officer (ISSO).

Contact

For further assistance with password issues, please contact the eRA Help Desk Monday-Friday 7am-8pm Eastern Time at:

- Web: http://ithelpdesk.nih.gov/eRA/
- Phone: 301-402-7469; Toll Free: 866-504-9552

Issue Date and Revision History

Rev #	Date	Change Description
0.1	6/1/07	Initial draft issued
0.11	3/17/09	Last Revision