Password Policy for eRA Applications

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.

Cancellations
This policy supersedes the following:

- Password Policy for Internal eRA Applications (March 2009)

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: ! # $ % - _ = + < >*

NOTE: The following special symbols are not permitted in eRA passwords. @ ^ & ( ) | " \ ' { } [ ] : ; ` ? , . /

    - Passwords cannot contain username
    - First and last characters cannot be numbers

- **Changing Passwords:**
  - Passwords must be changed at least every 120 days and the password cannot be reused within eight years (24 password cycles.) 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 within a 60-minute period. Lockout will last for 30 minutes or until reset by an authorized administrator.

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.

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:
Storing passwords in files on the user's system is prohibited. 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 Service Desk. Please see contact information below.

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

- Web: https://grants.nih.gov/support/
- Phone: 301-402-7469
- Toll Free: 866-504-9552