Passphrase Policy for eRA Applications

Purpose and Scope

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

Cancellations

This policy supersedes the previous Password Policy for eRA Applications

Applicability

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

Policy

NIH is moving from passwords to passphrases, effective November 9, 2021. Passphrases must contain at least 15 characters. Users who reset passwords for any reason (expiration, forgotten password, etc.) must create a passphrase that meets the new requirements.

Note: A passphrase is a memorable series of random words that does not need to contain numbers, capital letters, or special characters. To protect your account, your passphrase must not include your name, address, phone number, or any other information that is easy to guess.

Strong passphrase requirements

Passphrases **are required to be at least fifteen (15) characters in length** and must meet these requirements:

- **Simple**: You do not need to use special characters, numbers, or capital letters, though they are allowed as well as spaces.
- **Memorable**: Use a passphrase that is easy to remember but hard for others to guess.
- **Hard to guess**: Do not include personal information such as name, Social Security number, date of birth, HHS ID, etc.
- **Unique**: Weak and overused terms such as "password" will be rejected, and current or past passwords from work or personal accounts are not allowed.

Changing Passphrases

Passphrases must be changed at least once a year and cannot be reused within 10 passphrase cycles. Users must change their newly assigned password to a passphrase right after the first time they log on with their assigned password.

Account Lock-out

eRA modules will lock out a user account after 5 consecutive failed login attempts within a 120-minute period. Account would have to be reset by an authorized administrator.

User Session Inactivity

The module will disconnect user sessions that are idle longer than 45 minutes.

Caching Passphrases

Users are prohibited from caching (auto-saving) passphrases on the local system. Users must enter the passphrase at each login.

Sharing Passphrases

Users are prohibited from sharing passphrases with one other and each user must have a separate and unique passphrase. Users should not allow other unauthorized users to access resources under their credentials by logging on and then letting others use the computer.

Password Distribution and Storage

Storing passphrases in files on the user's system is prohibited. Passphrases must be stored, transmitted, and distributed in a secure manner. Passphrases must not be displayed on the screen when entered. Electronically storing or transmitting passphrases in plain text is prohibited.

Audit

Accounts and their adherence to the passphrase policy will be audited periodically.

Compromised Passphrases

Compromised passphrases 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 7 a.m. – 8 p.m. Eastern Time at:

- Web: https://era.nih.gov/need-help
- Phone: 301-402-7469
- Toll Free: 866-504-9552