eRA User Password Guide for IMPAC II Applications

Basic eRA Password Policy for Users

- Passwords will expire every 180 days.
- At expiration, users will have a 10-day "grace period" in which they will be reminded by the system as they log on that it is time to change their passwords.
- Inactive accounts (those associated with passwords that have been expired for more than 45 days) will be locked and will need to be unlocked by an IC Coordinator or IC User Admin before the account can be used.

Where and How to Change Passwords

- During the "grace period," each time a user logs on, he/she will have an opportunity to go to the "Change Password" module.
- If the user does not change their password by the end of the "grace period," the user will be forced to go to the Change Password module before logging on to any eRA system.
- Users can go directly to the "Change Password Module" at any time to change their password.
- The URL for the Password Module is http://impacii.nih.gov/webapps/.

Password Standards

- Passwords must be a minimum of 8 non-blank characters long.
- Passwords must contain at mix of letters, numbers and special characters.
- Passwords must contain at least one of the following special characters and these are the only special characters that are allowed:

  ! # $ % - _ = + < >

- Passwords may not begin or end with a number.
- Passwords may not contain the user name.
- Passwords may not be reused within one year.
- Passwords are not case-sensitive.
- Accounts will be locked after 5 unsuccessful login attempts. Accounts will also lock from the "Change Password" screen if a user attempts to change his/her password more than 5 times with an incorrect "old" password.
- Accounts can be unlocked by IC Coordinators or the IC Accounts Administrator in the User Admin Module.
- Passwords reset by IC Accounts Administrators or the Helpdesk will expire immediately and the user will need to reset password upon first login.

Notes on Implementation

Below is the schedule for the initial expiration of user passwords. Due to some issues associated with the rollout, some users may not get the "grace period" upon initial expiration. Also, some users who have recently changed their passwords may be forced to change them again. We are trying to avoid these situations but we may not be able to in some cases.

User Name begins with:	Password expiration date
A–C	December 10, 2003
D–L	January 7, 2004
M–P	February 11, 2004
Q–Z	March 10, 2004

The responsibility for maintaining user accounts, unlocking accounts, resetting passwords, etc., is normally that of the IC eRA Coordinator and/or IC Accounts Administrators. However, during the rollout period, for these policy and system changes, users can contact the eRA Helpdesk directly for assistance (helpdesk@od.nih.gov, 301-402-7469, 1-866-504-9552).