October 28, 2003

eRA Password Policy
Update for eRA Project Team

For additional details, see the eRA Password Policy document posted on the eRA web site at http://era.nih.gov/docs/NIH_eRA_Password_Policy.pdf

Background and Scope

- The eRA security audit revealed 11 password issues that must be addressed.
- eRA is a major application that contains sensitive data.
- eRA must adapt strong passwords to correct audit issues.

This policy applies to all users who access eRA servers and databases (IMPACII and Commons), including development and test servers and databases, as well as the personal workstations used to access these servers and databases.

Policy Basics

- Users must change their passwords at least every 180 days.
- Password length must be at least eight (8) characters.
- The password must contain a mixture of letters, numbers and special characters.
- The first and last characters cannot be numbers.
- The password cannot contain the user's login name.
- Passwords cannot be reused for a period of one year.
- The account will be locked after five (5) consecutive unsuccessful login attempts.
- Unless created by the user, initial passwords are pre-expired.
- Accounts associated with passwords that have been expired for more than 45 days will be deleted unless there is a *business reason* to retain them. *

*Initially we will do this deletion manually and contact each IC for coordination. Commons accounts (PIs, AOs, SOs, Reviewers) and ECB Council Member accounts will not be deleted for inactivity.

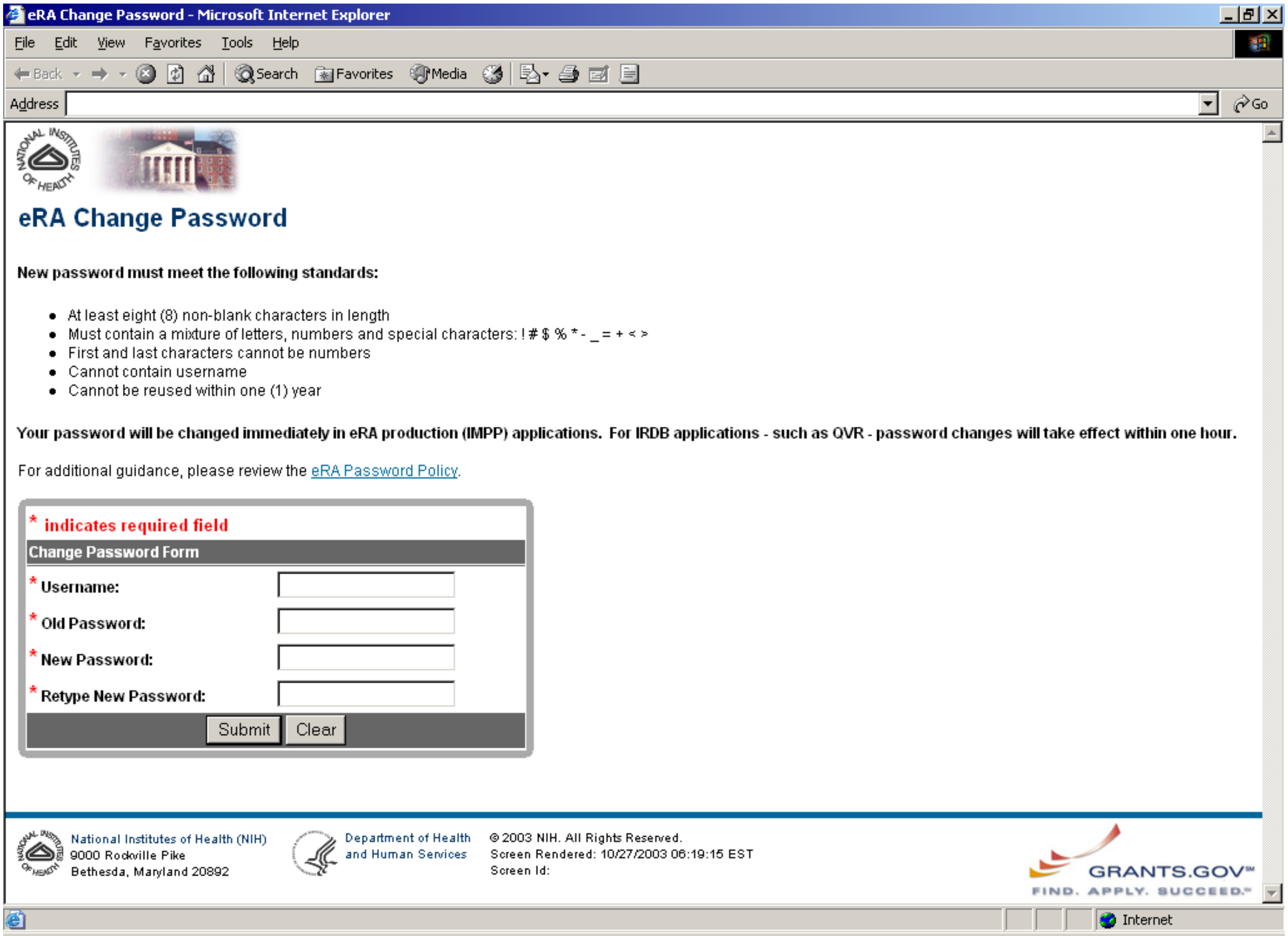
Application and User Impact

Ten days before a User's password is set to expire, user will get an expiration warning upon login. This warning will allow the user to change their password immediately or bypass and login. If passwords are not changed before expiration, users will be forced to change password before logging into eRA systems. Users with locked accounts cannot login until account is unlocked by an IC Account Administrator (via the User Admin Module).

eRA User Support/Analyst will be emailing Link account owners 20 days before password expiration to alert them to the change. Most Link account usernames begin with Link% so the majority will be expiring January 7, 2004.

All eRA applications will include the ability for a user to change their password. This will be a new enhancement for the internal J2EE applications like Grants Closeout Module, CM Web, Program Module and WebQT.

A stand-alone J2EE password change tool will be deployed. This will be the same password change page called from all eRA internal applications (J2EE and client server) for password changes. This stand-alone page may also be used for changing Link accounts passwords or called from IC extension systems for user password changes. The production url for this page will be http://apps.era.nih.gov/eraservices This tool changes passwords in the production database (IMPP IMPPRD). No application will support direct password changes in IRDB. Passwords will be changed in IMPP and bridged hourly to IRDB (as is the current practice). Sample of eRA Change Password:


eRA Change Password - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Internet

eRA Change Password

New password must meet the following standards:

- At least eight (8) non-blank characters in length
- Must contain a mixture of letters, numbers and special characters: ! # $ % * - _ = + < >
- First and last characters cannot be numbers
- Cannot contain username
- Cannot be reused within one (1) year

Your password will be changed immediately in eRA production (IMPP) applications. For IRDB applications - such as QVR - password changes will take effect within one hour.

For additional guidance, please review the eRA Password Policy.

* indicates required field

Change Password Form

* Username:	
* Old Password:	
* New Password:	
* Retype New Password:	

Submit Clear

National Institutes of Health (NIH)
9000 Rockville Pike
Bethesda, Maryland 20892

Department of Health and Human Services

© 2003 NIH. All Rights Reserved.
Screen Rendered: 10/27/2003 06:19:15 EST
Screen Id:

GRANTS.GOV™
FIND. APPLY. SUCCEED.™

Expiration dates will be enforced for existing IMPACII accounts. If a user's password has been changed within the past 6 months, the existing expiration date will be retained. For accounts where passwords have not been changed in more than 6 months, passwords will be expired according to the rollout listed below. To reduce impact, expirations will be phased in over a 6-month period. Password expirations will be grouped by first letter of Username as follows: A – D would expire November 19, 2003; E – H would expire December 10, 2003; I – L would expire January 7, 2004; M – P would expire February 11, 2004; Q – T would expire March 10, 2004; U - Z would expire April 7, 2004.

For Password Policy questions, contact Dave Carter, eRA ISSO.
For implementation questions, contact Tracy Soto, eRA Analyst/Deputy Enterprise Applications Architect.