PASSWORD POLICY FOR eRA
July 17, 2003

1.0 Purpose

This policy is intended to reduce the risk of unauthorized access to servers and databases essential to the mission of eRA. It defines:

- strong password standards
- password lifetimes
- guidance for password policy verification
- guidance for the establishment of passwords and modification of passwords
- Compliance and enforcement procedures

This policy addresses the risk of weak passwords as well as password disclosure – intentional or unintentional, malicious or benign – and hence, unauthorized access to servers and data.

2.0 Background

It is a well-established principle of IT security that strong passwords are an important part of any organization's security posture. Weak passwords can lead to unauthorized access. Such access would threaten the information whose integrity is essential to the mission of eRA and the National Institutes of Health. Easily guessable passwords are one of the most common ways to accomplish unauthorized access to any system. The National Institute of Standards and Technology suggests several ways to assist in the mitigation of the risks associated with unauthorized access by using better password policies in their document Generally Accepted Principles and Practices for Securing Information Technology Systems, URL; http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. NIST suggests that organizations clearly specify required password attributes. These should include minimum and maximum lengths, the type of characters that are acceptable, and contextual criteria. NIST goes on to suggest that passwords should be changed periodically and that users should be trained in good password selection.

3.0 Related Documents

NIH Password Policy, http://irm.cit.nih.gov/policy/passwords.html
NIH Guidance for Good Passwords,
http://irm.cit.nih.gov/policy/passwords.html

DHHS Automated Information Systems Security Program Handbook, http://irm.cit.nih.gov/policy/passwords.html
DHHS Personnel Security Suitability Program, http://www.hhs.gov/ohr/manual/98_1.doc

4.0 Scope

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

5.0 Policy

Unless specifically stated otherwise, the items in this section apply to both end user and system level accounts and passwords.

5.1 Requirements

- Each user must have a unique username.
- Each IC through a Memorandum of Understanding (MOU) will accomplish suitability determination for each end user.
- Initial passwords must be communicated to the user securely.
- Unless created by the user, initial passwords are pre-expired.
- Passwords for system level accounts, application administrative accounts, system administrator accounts, and database administrator accounts:
    - Must be changed at least every 90 days.
    - Initial password must be changed by logging into the system within 5 days of issue.
- End user passwords must be changed at least every 180 days.
- Accounts associated with passwords that have been expired for more than 45 days will be deleted unless there is a business reason to retain the account, e.g. principal investigator that logs on once or twice a year.
- Authentication must be to individual users, not groups.
- No passwords are to be stored in clear text.
- No password will be given to a user, an account unlocked, or a password changed without the identity of the user being properly validated by the Account Administrator.

5.2 Password Guidance

- The password cannot contain the user's own or close friend's or relative's name, employee number, social security number, birthday, significant anniversary, telephone number, address, or any other information about the user that could be easily guessed or discovered.
- Passwords must not contain common words or words found in any dictionary.
- Keyboard patterns cannot be used, e.g. qwerty.
- Passwords must be changed immediately if they have been given to someone else.
- To prevent accidental disclosure the following precautions must be taken:

    - Passwords must not be disclosed to anyone, including anyone claiming to be User Support Branch Staff or high ranking eRA management.
    - Passwords must be stored in an encrypted form on any file, including a PDA.
    - Users should not communicate his/her password or password paraphrase in an email.
    - Passwords should not be written down.
    - New passwords cannot be a simple change of the previous password, e.g. adding a number at the beginning or end, changing one letter or number.
- The Principle of Least Privilege must be used in assigning privileges to accounts.
- Same username should have unique passwords across environments.

5.3 Password Formulation Standards

- Password length must be 8 or greater characters.
- Must contain a mixture of alpha and numeric characters, as well as special characters.
- The first and last characters must not contain numbers.
- The password cannot contain the user's login name.

5.4 Password Change Requirements

- Passwords cannot be reused for a period of one year.
- Passwords must be changed as soon as possible after a compromise and within one business day.

- A password must be changed if directed to do so by User Support Branch Personnel.

5.5 Protecting Passwords

- The account will be locked after 5 consecutive unsuccessful login attempts as specified in the procedures associated with this policy.

6.0 Responsibility

The User Support Branch (USB) acts as the point of contact for the NIH Office of the Director (OD) and the Division of Extramural Information Systems (DEIS) for all users requiring new accounts, roles, password changes, and the reporting of possible compromises as well as any other issues involving user accounts. For all other ICs and OPDIVS this authority is delegated to the eRA/IMPAC II Coordinators within that IC/OPDIV who can in turn delegate the actually management of accounts and access to the User Admin Module to IC/OPDIV staff as appropriate. Requests for IC/OPDIV staff access to the User Admin Module must be made by the eRA/IMPAC II Coordinator in writing (email acceptable) to USB. IC/OPDIV accounts will be reviewed and validated by the USB at least annually. The USB also acts as a liaison between the user and the System Operations Management Branch (SOMB). The USB works with IC and Institution staff to ensure that accounts are closed on all relevant servers and applications where a user account is no longer needed.

The Systems Operations Management Branch (SOMB) sets up user accounts according to this policy when contacted by USB. No new account is established until the user has signed a user policy form that has been validated by the Accounts Administrator.

The Information System Security Officer (ISSO) is responsible for ensuring that this policy is followed. She/he is also responsible for all changes to this policy. The ISSO is responsible for auditing the compliance with the policy. The ISSO makes recommendations for modifications that it deems necessary to the eRA management.

Users are responsible for protecting their passwords and reporting any compromise promptly to the USB. They are also responsible for selecting strong passwords.

Management is responsible for ensuring that users are aware of this policy. They also must be consistent in the enforcement of this policy.

7.0 Compliance

All servers have the Operating System configured to enforce this policy. The USB does periodic "social engineering" checks to ensure that users do not divulge passwords. Users who repeatedly choose weak passwords are subject to either restricted access or possible disciplinary action if they choose weak passwords for four consecutive months.

8.0 Enforcement

If identified password policy violations are not corrected within one business day, the account is locked. If repeated violations occur, the employee is subject to termination. Management ensures the uniform enforcement of this policy.

9.0 Revision history

This is a new policy. There is no existing policy that is made obsolete by this policy.

/s/James Cain
Director, DEIS

_____
Date