NIST Information Technology Security Management Handbook

Passwords Policy

Status Purpose Scope Background Policy Responsibilities
Exemptions

Status: Approved

Revised: December 30, 2003

Purpose

This document states the National Institute of Standards and Technology (NIST) policy, and provides guidance, on the management and use of passwords to control access to NIST Information Technology (IT) resources. The goal is to establish strong and consistent password practices to prevent unauthorized access to NIST IT resources.

Scope

This policy applies to employees, contractors, contractor employees, guest researchers, collaborators and others having access to and/or use of NIST IT resources.

This policy addresses IT security requirements for all NIST IT systems and networks, independent of the size of the computer or network. For example, it includes desktops, laptops, personal digital assistants (PDAs), other handheld devices, etc. It also applies to IT systems used to support NIST that are operated by contractors, guest researchers, collaborators, and other Federal agencies, including IT systems not owned by NIST but located on NIST property or connected to NIST networks. This policy must be explicitly addressed in all IT procurement activities except for those systems intended to provide unrestricted access (e.g. web pages).

This policy addresses the establishment, implementation, maintenance, and enforcement of passwords used as a form of user authentication and access control. The management and use of other forms of user authentication (e.g. one-time passwords, public key cryptography, etc.) are outside the scope of this policy.

Background

NIST provides access to its IT resources to solely support the missions of NIST, the Department of Commerce, and the U.S. Government. NIST is required by Federal regulations to establish effective controls to prevent unauthorized access to NIST resources, and to effectively monitor and detect such attempts.

The use of passwords is the most commonly used form of user authentication to control access to NIST IT resources. Passwords are one of the weaker forms of user authentication. To provide adequate protection for NIST IT resources, it is necessary for each user to select strong, complex passwords, change passwords periodically, and never share passwords.

Policy

1. Passwords should only be used when no stronger form of user authentication and access control mechanism is available. For example, one-time passwords and public key cryptography should be used instead of password authentication if possible.
2. Passwords must be generated or selected using the following criteria:

   (1) a. All passwords must have at least eight (8) non-blank characters.

   (2) b. At least one of the characters must be a number (0-9) or a special character (e.g. ~, !, $, %, ^, and *)

   (3) c. No character may be repeated more than four (4) times

   d. Passwords used to control privileged or administrative access must be different than passwords used to control general access on any given system.

   (4) e. Passwords must not include control characters and non-printable characters (e.g. enter, or tab, or backspace, or ctrl-c, etc.).

   (5) f. Passwords must not include any of following: vendor/manufacturer default passwords, names (e.g. system user names, family names), words found in dictionaries (i.e. words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g. 3456, ghijk, 2468).

   g. Passwords may be created using random password generators.
3. All passwords must be protected to prevent unauthorized use:

   (6) a. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an approved NIST IT system security plan. Once shared, passwords must be changed as soon as possible.

   b. Group passwords (i.e. a single password used by several users) should be used with some other mechanism that can assure accountability.

   c. Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized.

   d. Group passwords must not be used for access to other applications, and they must never be re-used.

   e. Passwords in readable form must not be left in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password.
   f. Passwords for user authentication must not be stored in readable form in batch files, automatic login scripts, software macros, keyboard or terminal function keys.
   g. The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.
   h. User applications must not be enabled to retain passwords for subsequent reuse.
   i. Passwords must not be distributed by non-encrypted email.
   j. Passwords must not be distributed through phone mail.
   k. If sent by regular mail or similar physical distribution system, passwords and user IDs must be sent separately.
   l. Passwords for access to NIST systems must not be the same as passwords used for access to Internet systems or systems not on NIST networks.
   m. Access to password files or password databases must be restricted to only those who are authorized to manage the IT system.
   n. If authorized access would be prevented if the password were lost or forgotten, then the password must be documented and stored in a restricted, secure area (e.g. Division office safe or locked file cabinet). Access to these passwords must be restricted to authorized personnel for purposes of maintenance and contingencies.
   o. Passwords should be encrypted when transmitted across any network. However, passwords must be encrypted when transmitted across the Internet. This requirement does not apply to single-use (one-time) passwords.

4. All passwords must be changed as follows:
   (14) a. Passwords must be changed as follows:
      i. At least every ninety (90) days,

      (15) ii. Immediately if discovered to be compromised or one suspects a password has been compromised,

      (16) iii. Immediately after being shared for emergency purposes,

      (17) iv. Immediately if discovered to be in non-compliance with this policy, and

      (18) v. On direction from management.

   (19) b. Passwords must not be reused for two (2) years, nor can any of the last eight (8) passwords that have been used be reused.
   (20) c. All vendor supplied default passwords must be changed as soon as possible and before the respective IT resource is connected to a NIST network.
5. All passwords must be administered as follows:
   a. After no more than four (4) failed attempts to provide a legitimate password for any access, the request should result in the failed attempts being recorded in an audit log and:
      (21) i. Access immediately suspended, and then automatically restored following a predetermined time period, not shorter than three (3) minutes or to be restored by a systems administrator; and

      ii. The user being immediately disconnected from the service if access is provided by a network or dial-up service.

   b. Automated mechanisms, utilities, and software should be used to ensure that password selection, verification, use, and management are implemented and in compliance with this policy.

   c. Access to password files or password databases must be restricted to only those who are authorized to manage the IT resource.

   d. Users must be notified immediately to change their password if it is suspected their password may have been compromised or discovered to not be in compliance with this policy. If the password is not immediately changed, the account must be temporarily suspended until the password is changed.

6. Additional password restrictions and criteria are permitted as long as they continue to be in compliance with this policy and are adequately documented in an approved NIST system security plan. This documentation must also include the reasons why additional restrictions and criteria are necessary.

Exemptions

All requests for waivers to this policy must be reviewed and approved by the Director of the OU responsible for the system, the NIST ITSO, and the NIST Chief Information Officer (CIO), after which they will be submitted to the DOC IT Security Manager for final approval. This waiver must:

1. cite the specific mandatory practice(s) for which the waiver is requested,

2. explain the rationale for the requested waiver, and

3. if applicable, describe compensating controls to be in place during the period of the requested waiver, until systems are compliant with this policy, and provide an action plan (including target dates) for compliance.

Approved waivers must be documented as part of the relevant system’s security plan. Identical sub-systems under the same management authority and covered by one system security plan require only one waiver request.

For those systems that need to be modified or enhanced to be compliant with this policy, the NIST IT System Security Plan must also include an action plan with milestones for when the system will become either fully or partially compliant.

Responsibilities

All NIST Operating Units (OUs) must ensure that the management and use of passwords to control access to NIST IT resources are in compliance with this policy. The OU's Director is responsible for ensuring compliance with this policy within their OU.

The NIST IT Security Officer (ITSO) will ensure the communication of this policy to all IT users by addressing password management within the IT security awareness and training program. The NIST ITSO will also periodically monitor for compliance with this policy.

System owners and system administrators are responsible for implementing procedures and mechanisms necessary for the implementation and enforcement of this policy.

Users are responsible for all activities involving the use and safeguarding of their passwords.

Date created: December 30, 2003
Last updated: December 03, 2007
Inquiries/Website Comments: OCIO_ITSD_Webmaster@nist.gov