National Institute of Standards and Technology
Business Systems Division

NIST Commerce Purchase Card System User Access Authorization

This form must be completed in order to obtain access to the NIST Commerce Purchase Card System (CPCS). Please complete the user information block below. In order to be accepted, this form ***must be signed by you and your supervisor***. You may not sign your own form**.** Send completed form to:

Teresa Coppolino
100 Bureau Drive
Building 222, Room A203, STOP 3740
Gaithersburg, MD 20899-3740

Direct questions to the Customer Interaction Center at (301) 975-6100.

Name: _____

Title: _____

Bureau/Division: _____

Address: _____

Email: _____ Phone Number: _____

CPCS Function: _____

In addition, all applicants for an account on the NIST Commerce Purchase Card System must read the attached statements on NIST central computing security, password management and record retention policies. Sign below to indicate that you agree to abide by these policies. Applicants who fail or refuse to sign below or who fail to abide by the security, password, and record retention policies will be denied access to the NIST Commerce Purchase Card System. Your supervisor must sign below.

I acknowledge receipt of the statement of NIST central computing security policies and understand that I am expected to abide by the user responsibilities defined in that statement.

Applicant Signature: _____ Date: _____

Supervisor Approval: Printed Name: _____

Signature: _____Date: _____

For Use by the NIST Business Systems Division

Username: _____ New Account: Y / N

User Function: [ ] Cardholder [ ] Approving Official
[ ] Initiator [ ] Group Administrator
[ ] Finance [ ] System Administrator
[ ] Procurement [ ] Other _____

Business Systems Division Approval:

Signature: _____ Date: _____

Completion Date: _____ By: _____

NIST Policy on
Information Technology Resources Access and Use

October 8, 1998

NIST provides staff and collaborators access to information technology resources, including computers, networks, and peripheral devices, to support the NIST mission. The following guidelines apply to all who use and access NIST information technology resources.

Acceptable Use of NIST Information Technology Resources

This section describes use of NIST information technology systems that are considered acceptable by NIST management. The general criteria used in deciding acceptable use are whether the application is of benefit to NIST, whether it complies with government laws and regulations, and whether it does not adversely affect others. NIST allows the personal use of the Internet as long as it does not interfere with official business, increase cost to NIST or embarrass NIST. Questions about the use of NIST information technology resources that are not explicitly mentioned in this policy should be directed to NIST management.

NIST information technology resources may be used in the conduct of NIST research, in the administration and management of NIST programs, and in the dissemination of the results of NIST work. Examples of such use of NIST information technology include, but are not limited to:

- Computation, modeling and simulation, and support of experiments needed to accomplish NIST research, including research on information technology systems;
- Analysis and storage of data, including experimental data, output from models, and administrative data;
- Visualization of the output from models and experiments;
- Preparation of reports, papers, memos, correspondence, databases, graphics, displays, presentations, and any other products of NIST work;
- Management of NIST operations and staff.

NIST information resources may be used to communicate and exchange information with others located at NIST, and elsewhere, to share information related to the NIST mission. This includes researchers at other institutions, customers in industry, and elsewhere, vendors and companies with products of interest to NIST, other government agencies, and the public. Examples of acceptable communications include:

- Disseminating appropriate information related to NIST mission topics electronically to our customers in industry, government, universities, and the public around the world;
- Communicating by electronic mail or other means with research colleagues, customers, other government agencies, and vendors for purposes of NIST business;
- Accessing public information available on the Internet, or elsewhere, related to NIST research and the mission of NIST;
- Obtaining software patches, and updates from vendors, public domain software repositories, and other sources, provided such software is obtained, checked and tested, and installed in accordance with U.S. copyright regulations, the license for that software, and NIST security policies;
- Participation by NIST employees and collaborators in forums, news groups, and other information exchanges for the purpose of furthering the NIST mission or improving the professional knowledge or skills of NIST staff.

Acceptable Access to Information Technology Resources

NIST communications facilities may be used to provide access to NIST information technology systems and those of other organizations for authorized purposes. Examples of authorized access to systems include:

- Access to NIST systems and networks from off-site locations for NIST employees and collaborators with specific needs for such types of access, such as access when on travel or from home;

- Access for NIST staff and collaborators to academic, government, and industrial computer systems for accomplishing joint projects, where that access is authorized by the owner;
- Access to academic computing facilities for use by a NIST employee taking courses.

To ensure accountability of actions and resources, each person who has access to a NIST information technology system must have an individual account. Sharing of accounts and passwords or authorization methods is prohibited, except in special cases such as e-mail accounts for the operation of special services supported by a team of people.

Access to NIST information technology resources by employees and non-employees require formal written authorization by a NIST manager. The authorization should specify the duration of the access to the NIST resource, acceptable use of the NIST resource, and a rationale for granting access to NIST information technology resources. A copy of the authorization and a copy of this policy should be given to the user. Use by users may be subject to suspension or discontinuation without notice if it impairs other activities. Non-employees (collaborators) requiring written formal authorization prior to granting access to NIST information resources include:

- Guest researchers, contractors, emeritus employees, and others with a formal relationship with NIST;
- People who do not have a formal relationship to NIST, but who are involved in cooperative work with NIST staff.

Non-employees who access NIST information technology resources, such as Web, bulletin boards, public anonymous ftp, Mosaic, gopher, or other services used by NIST to disseminate information to the public need no special authorization. However, misuse of these services or attempts to exceed authorized access is subject to the same sanctions as other unacceptable uses described below.

Unacceptable Use of NIST Information Technology Resources

The use of NIST systems and networks in a manner which is unacceptable may subject the person(s) involved to loss of all privileges to use NIST systems, may result in other disciplinary sanctions up to and including dismissal, or may result in criminal prosecution. Unacceptable uses of NIST systems and networks include, but are not limited to:

- Commercial or business use for the profit of an individual, or company, or other use of NIST systems not approved by a NIST manager as essential to the NIST mission;
- Any use of NIST information technology resources in order to obtain access to any network or system at NIST, or elsewhere, for which the person has not been authorized, or in a manner that knowingly violates the policies of the owner of the network or system;
- Any activity that interferes with the legitimate activities of anyone using any NIST systems or networks, or any other network or system which may be accessed from NIST;
- Unauthorized use of a system for which the user has authorized access, including use of privileged commands on a system by a user not authorized to use such commands and unauthorized access to information owned by someone else. For example, no user may access the root account on a Unix system or attempt to become root on the system unless he or she is authorized to do so;
- Deliberate unauthorized destruction of NIST data or other resources;
- Any use of NIST information technology resources to engage in illegal or unethical activities;
- NIST expects employees and collaborators to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or the public. Such as e-mail that contains (a) political statements, (b) religious statements, (c) cursing or other foul language, (d) pornographic information and (e) statements viewed as harassing others based on race, age, creed, color, sex, physical handicap, or sexual inclination;
- The unauthorized sharing of NIST-owned software or any other NIST information not authorized for disclosure or use by others with anyone not specifically authorized to receive such software or information.

Privacy of Information

NIST systems and any information on those systems are Government property. Therefore, all employees and users of NIST systems should be aware that information transmitted by or stored on

NIST systems is not private. In addition, NIST users should also be aware that it is often necessary to monitor network traffic or computer activity to ensure integrity, security or reliable operation of NIST systems. However, any other monitoring of employees' communications is against NIST policy. Casual reading of e-mail messages addressed to others is prohibited.

After reading the NIST computer security policy please sign the signature page to verify that you have read and will abide by this policy.

Contact mailto:nist-itso@nist.gov?subject=Internal ITS Web Inquiry for additional information
Last updated:08/06/02
Date created: 07/22/2002

(Keep this memorandum for your records)

February 26, 2001

MEMORANDUM FOR NIST Central Computing Facility Users

From: Ray Hoffmann, Chief
Information Services and Computing Division

Subject: Central Computing Security Policies

As a user of NIST central computing services, you are expected to be aware of and abide by the security policies and procedures covering the NIST central computing facilities. Please read and retain the following statement of policies and procedures. Also, complete and return the attached acknowledgement memorandum that will be included in our records concerning your use of the facilities.

NIST central computing services are provided by the Scientific Computing Facility sites in Gaithersburg and Boulder, and the Management Information Computer Facility (MICF) in Gaithersburg. In managing those facilities, High Performance Systems and Services Division (HPSSD) must meet the requirements of various Federal computer security regulations and guidelines, such as OMB Circular A-130 and the Department of Commerce Information Technology Management Handbook. HPSSD has developed a computer security plan for each facility as required by the Computer Security Act of 1987, conducts periodic risk analyses, and maintains a disaster recovery plan for continuing computing services to our customers in case of an extended outage of the computing facilities.

AUTHORIZED USAGE

1. NIST central computers shall be used for official Government work only.
2. A valid NIST cost center must be associated with each user identification (userid), so the resources used under that userid can be traced to a valid NIST task.
3. HPSSD will periodically confirm the validity of cost centers and the identity of individuals associated with central computing userids.

CLASSIFIED/SENSITIVE INFORMATION

1. No classified or sensitive information shall be processed or stored in NIST Scientific Computing Facility systems or associated storage facilities.
2. Records subject to the Privacy Act and other sensitive information may be processed and stored on the MICF. The owner of such information is responsible for ensuring that it is adequately protected and accessible only by those personnel with a valid authority to see or use it.

ACCESS CONTROL

1. Each user of a NIST central computing system shall have a personal userid and associated password. The userid/password must not be shared. Users will be held personally responsible for problems arising through the use of their userid/password.
2. Each user is responsible for protecting and maintaining his/her password. Care shall be taken in selecting and using a password to ensure that it is not easily guessed or disclosed. Where the computer system permits it, a password should be at least eight characters in length and a combination of numeric and alphabetic characters (upper and lower case). The password should be changed frequently, especially if there is a chance that it has been disclosed.
3. HPSSD shall implement and maintain procedures that require passwords to be periodically changed (currently every 3 months).
4. HPSSD manual account maintenance procedures shall not require a user to disclose his/her password, and shall not permit HPSSD staff to overwrite or change an existing user password without confirming the identity and authority of the person requesting such a change.

INFORMATION PROTECTION

1. HPSSD shall:
   - maintain physical access controls, environmental controls, and fire suppression systems to protect the contents of NIST central computing facilities;
   - configure operating systems so that files created on NIST central computers are accessible, by default, only to their owners;
   - make periodic backup copies of permanent disk files for use in recovery from computing system failures or a computing facility disaster; - arrange for the off-site storage of copies of disk files and magnetic tapes for users whose applications require an extra level of protection from a possible computing facility disaster;

- maintain procedures for the movement of backup files and materials to alternate computer sites in case of a disaster; and
- provide special handling for sensitive output materials to prevent their inadvertent release to unauthorized recipients.

2. Each central computing user shall:
   - have the ultimate responsibility for determining the appropriate level of protection for his/her information processed and stored in NIST central computing facilities;
   - notify HPSSD if the security policies identified in this document do not provide an adequate level of protection for his/her applications and associated information;
   - make special arrangements with HPSSD for handling sensitive output materials or for producing copies of any disk files, magnetic tapes, or other materials to be stored off-site;
   - exercise great care in moving software or data from outside sources onto NIST central computing systems so as to guard against the possible introduction of a computer virus or other threat.

AUDITING COMPUTING RESOURCE USAGE

1. HPSSD shall:
   - monitor the use of central computing resources, investigating unusual usage levels and patterns to ensure against unauthorized or inappropriate use;
   - maintain a collection of information which identifies the central computing resources used under each userid;
   - issue periodic reports to user management on computing resources consumed by users associated with their cost centers;
   - provide special reports, upon request, to management and users; and
   - notify users in a timely manner about any known loss or compromise of information processed and stored in NIST central computing facilities.
2. Each user cost center manager shall:
   - review or arrange for review of computing resource usage reports by management officials able to judge appropriate levels of usage; and
   - notify HPSSD immediately about any unusual or unexpected usage under the cost centers for which he/she is responsible.

VIOLATIONS OF NIST COMPUTER SECURITY POLICIES MAY RESULT IN WITHDRAWAL OF THE PRIVILEGE OF USING NIST CENTRAL COMPUTING RESOURCES AND IN OTHER DISCIPLINARY ACTION AS DESCRIBED IN THE NIST ADMINISTRATIVE MANUAL.

(Keep this memorandum for your records)

NIST Policy on the Management and Use of Passwords to Control Access to Information Technology Resources

1. Purpose

This document states the National Institute of Standards and Technology (NIST) policy on, and provides guidance on the management and use of fixed and secret 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.

2. Contents

3. Information and Assistance

Guidance on this policy may be obtained from:

NIST IT Security Office
NIST
Mail Stop 8901
301-975-2901

4. Definitions

Access Control	Mechanisms and policies to restrict access to IT resources
Administrative Access	Advanced level of access to a computer or application that includes the ability to perform significant configuration changes such as changes to the computer's operating system. Also referred to as privileged access.
General Access	Normal or basic level of access to a computer or application that allows only minimal configuration changes. This level of access is the most common way used to access a computer or application.

NIST System Security Plan	NIST document which describes management, technical and operational controls of a system, current and planned.
One-time Passwords	A string of characters used to authenticate a user and provide access to an IT resource that becomes invalid after it is used the first time.
Password	A fixed, secret string of characters used to authenticate a user and provide access to an IT resource more than once.
Public Key Cryptography	A method for creating and exchanging secret messages and performing strong authentication without two (2) parties or systems having to share the same secret password.
System	A set of computers, processes, applications, and related IT resources that are under the same direct management control; have the same function or mission objective; have essentially the same operating characteristics and security needs; and reside in the same general operating environment.
User Authentication	A process for verifying the identity of an individual.
User-ID	A string of characters used to uniquely identify when accessing a system.
Must	Requirements that are mandatory for compliance.
Should	Requirements that are to be followed unless there is a technical or risk-based reason for an exception.

5. Background

NIST provides access to its IT resources to solely support the missions of NIST, the Department of Commerce, and the US Government. NIST is required by Federal regulations to establish effective controls to preclude unauthorized access and to effectively monitor and detect attempts to gain unauthorized use of NIST resources.

The use of fixed, secret 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 to select strong, complex passwords, change passwords periodically, and never share passwords.

6. Scope

This policy applies to all NIST Operating Units (OU) and other NIST organizational components that operate or use IT resources in support of NIST and Federal government programs. This includes employees, external DOC 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, and including all systems using automated technology where passwords can be used to control access. For example, it includes desktops, laptops, Palms, personal digital assistants (PDAs), and other handheld devices, etc. This includes those IT systems operated by contractors, guest researchers, collaborators, and other Federal agencies used to support NIST. This also includes IT systems not owned by NIST but located on NIST property or connected to NIST networks.

This policy addresses the establishment, implementation, maintenance, and enforcement of fixed, secret passwords used as a form of user authentication and access control. The management and use of other forms of user authentication mechanisms (e.g. one-time passwords, public key cryptography, etc.) are outside the scope of this policy. Except where otherwise noted in this policy, the two terms **password,** and **fixed, secret password** are used interchangeably.

7. Policy

(1) Passwords should only be used when no other 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.

(2) Passwords must be generated or selected using the following criteria:

a. All passwords must have at least 8 non-blank characters.

b. All passwords used to control general access must contain at least the following (NIST CPCS requires general access password).

1. one alphabetic character,

2. one numeric character,

c. All passwords used to control privileged or administrative access must contain all of the following.

1. one alphabetic character,

2. one numeric character, and

3. one non-alphabetic and non-numeric character (e.g !, %, &, etc.).

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

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

f. Passwords must not include words in dictionaries, user-IDs, derivatives of user-ID, and common character sequences (e.g. 3456, ghijk, 2468, etc.). Personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. Common character patterns, even in combinations such as xyz123ab, must not be used.

(3) All passwords must be protected to prevent unauthorized use.

a. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an approved NIST System Security Plan.

b. Passwords for group accounts are permitted but must not be shared outside the group.

c. Passwords for group accounts and passwords that need to be shared because of an overriding operational necessity must be unique and cannot be used for access to other applications.

d. 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.

e. Passwords for user authentication must not be stored in readable form in batch files, automatic login scripts, software macros, keyboard or terminal function keys.

f. 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.

g. User applications must not be enabled to retain passwords for subsequent reuse.

h. Passwords must not be distributed by non-encrypted e-mail.

i. Passwords must not be distributed through phone mail.

j. If sent by regular mail or similar physical distribution system, passwords and user-IDs must be sent separately.

k. 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.

(4) Passwords, for which authorized access would be prevented if the password were lost or forgotten, 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.

(5) All passwords must be changed as follows:

a. All passwords must be changed at least every six (6) months. More sensitive applications and systems may require a shorter interval.

b. Passwords must not be reused for two (2) years.

c. All passwords must be changed immediately after being shared for emergency purposes.

d. All passwords must be changed immediately after being compromised or if one suspects that a password has been compromised.

e. All passwords must be changed as directed by management.

f. All vendor supplied default passwords must be changed as soon as possible and before the respective IT resource is connected to a network.

g. All passwords must be changed if they are found to be in non-compliance with this policy.

(6) All passwords should be administered as follows:

a. After no more than five (5) 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:

1. Access to be 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

2. 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. Passwords should be encrypted when transmitted across a network.

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

e. 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.

(7) 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.

8. Responsibilities

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

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. The NIST IT Security Office will periodically monitor for compliance with this policy.

All requests for exceptions to this policy must be reviewed and approved by the Director of the Operating Unit responsible for the system and the NIST IT Security Office or NIST Chief Information Officer. Exceptions must be thoroughly documented in the respective NIST System Security Plan and must include the reason for the exception and all additional compensating and equivalent security precautions taken to prevent unauthorized access. For those systems that need to be modified or enhanced to be compliant with this policy, the NIST System Security Plan must also include an action plan with milestones for when the system will become either fully or partially compliant.

Signed: /WMehuron/ Dated: December 19, 2001

User Responsibilities for Printed and Electronic Media

Users are responsible for the storing, securing, archiving and deletion of printed material and electronic media obtained from the NIST Commerce Purchase Card System in accordance with DOC and other Federal policies on record retention and archiving.

MEMORANDUM FOR Business Systems Division
Attn: Rich McKay
Chemistry Bldg 222, Room A225 STOP 3740
Gaithersburg, MD 20899

From: _____
Name (printed or typed)

Subject: NIST Central Computing Security and Password Policies

I acknowledge receipt of the following statements: 1.) NIST Policy on Information Technology Resources Access and Use; 2.) NIST Central Computing Security Policies; 3.) NIST Policy on the Management and Use of Passwords to Control Access to Information Technology Resources; and 4.) User Responsibilities for Printed and Electronic Media and understand that I am expected to abide by the user responsibilities defined in each of these statements.

_____ _____
Signature Date