System Access Policy Compliance Standards for UNH

NOTE: The text in yellow highlight is the USNH System Access Policy and cannot be modified.

The bulleted entries under each policy section are suggested compliance standards that are under consideration and discussion. These standards will evolve in response to changing threats, improving technologies, and feedback from community and governance representatives. Readers should check back frequently to ensure currency of understanding the minimum standards.

Where compliance is not reasonably practical by the effective date, please contact it.security@unh.edu as soon as possible to discuss the situation, agree on next steps, and consider steps you can take to minimize the risks associated with the situation.

5.7.1 Control Access to Information. Computer systems and resources used for the transaction of USNH business shall be protected from theft, malicious destruction, unauthorized alteration or exposure, or other potential compromise resulting from inappropriate or negligent acts or omissions.

5.7.1.1 Computer systems shall require utilization of employee-specific passwords for access. Passwords for access to USNH systems shall comply with industry standards as established by the institutional Chief Information Officers within the technological capabilities of each system.

a) UNH information technology providers shall not issue shared accounts with shared passwords. Exception: In some instances of system/service/local accounts, employees have no choice but to share an account and password to be able to contribute and/or have redundancy to do their work because the existing technology does not allow for more than one system account. Those cases shall be documented for the CIO with a request for approval through it.security@unh.edu, and the employees shall have a signed confidentiality agreement on record. A request form and confidentiality agreement template is available from it.security@unh.edu and posted at http://cis.unh.edu/itsecurity. The password in question must be changed when one or more of the employees changes responsibilities or leaves their position.

b) Employees who previously shared passwords for one or more information technology account shall reset their password to ensure that others can no longer use their password.

c) Employees who have the apparent business need to share account names and passwords shall contact their information technology service provider so that alternate arrangements can be made within compliance of this policy. The solution may require a change to business processes.

d) UNH shall utilize secondary accounts to provide access (but not the accounts) to persons who are not approved for their own accounts but are

---

1 These standards were endorsed by the UNH Steering Committee for Information Technology (SCIT) April 29, 2009.
approved by data stewards and system administrators as having a legitimate business need to access certain computing environments under strict supervision.

e) Use of the root account to login to UNIX/*NIX systems is considered a dangerous practice because it does not provide a user audit trail where the root account is used by more than one person. Use the “sudo” (one-time substitute user) or “su” command instead, and only when root privileges are required. sudo/su provides a safer way for administrators on multi-user systems (as well as for users on home computers or other single-user systems) to use the system than to routinely log on as the root user. That is, there is much less potential for accidental or malicious damage if an administrator first logs on as an ordinary user (who, by default, has very limited system privileges) and uses that account for routine tasks that do not require root’s sweeping powers. sudo/su can then be used to switch to the root account for only those operations that actually require root access (e.g., making system repairs and managing user accounts).

In addition, not only the root account but also sudo/su should be used to the minimum extent necessary, and it should be used with great caution. Use accounts configured for the least privilege necessary to complete your work. This includes making certain (1) that no unauthorized persons see any passwords used with sudo/su (such as watching a password being typed in or seeing it on paper), (2) that sudo/su sessions are not left unattended and (3) that sudo/su sessions are terminated as soon as the tasks for which they were invoked have been completed.

Remote access methods on the UNIX/*NIX systems should be configured to not allow root account login. Configure SSH and other remote access methods to disallow direct root login, and use sudo/su instead. If a non-interactive (scripted) login is required, consider using SSH keys and avoid using solely passwords.

5.7.1.2. Password change schedules will be established and communicated to password holders at timely intervals.

a) The minimum frequency of password changes will be at least once every six months.

b) Passwords must be “strong”, at minimum with the following complexity:

- at least 7 characters
- at least 1 uppercase letter [A-Z]
- at least 1 lowercase letter [a-z]
- at least 1 digit [0-9]
- at least 1 special character such as: % * + - _ . , : ; / | = ? ! [ ] ^ ~
d) For any systems that currently do not support one or more of the above length or complexity standards, the remaining standards will apply.

e) Password(s) must not be based on anyone's name, personal data, or words that might be found in a dictionary (in any language). Note that passwords are case-sensitive, so you must remember which letters in your password are uppercase or lowercase.

f) IT Systems that have the technical option for enforcing the strong password and frequency standard shall be configured to do so.

g) UNH shall issue a general communication about the minimum change schedule for all university passwords to the campus community prior to the May 1 effective date of this policy.

h) Information technology service providers shall follow up with periodic reminders to their clients about required password changes.

i) Password expiration shall be enabled on those information technology systems that have such functionality.

j) Some systems do not currently have the settings to enforce password expiration; for these system enforcement capabilities will be added as the systems are upgraded or replaced.

5.7.1.3 Employee-specific passwords shall be treated as sensitive, confidential information and shall not be shared. Employee-specific passwords also shall not be stored on-line or written down unless adequately secured from unauthorized viewing.

   a) Employees who have shared passwords for one or more information technology accounts shall reset their password to ensure that others can no longer use their password.

5.7.1.4 Authorized users of computer systems will take reasonable and appropriate measures to prevent access to systems by unauthorized persons.

   a) Computer systems will be protected from physical theft using measures that are appropriate to the threat and the work environment.

   b) When not actively monitored, computer systems that are logged into one or more accounts will be protected from viewing and access by unauthorized persons. Such protection may be accomplished through solutions such as locking the session/screen, preventing physical access to the computer, and/or maintaining physical and visual control of the computer.

5.7.1.5 All data on computers or electronic storage devices (including but not limited to desktop, laptop, server, or handheld devices) shall be wiped clean of files and data prior to transfer or surplus.

   a) Transfer means relinquishing ownership or control of the machine (device and/or media) between persons and/or organizations.
b) Transfer does not mean temporarily giving the device and/or media to an internal UNH service provider, such as the CIS Computer Service Center, an Academic Technology Liaison, or another authorized technical support person for the purpose of supporting the owner of the machine. In these cases:
   - All restricted data should be deleted by the owner from the machine before giving the device and/or media to the service provider.
   - The service provider shall have on file with their senior leadership an agreement for each person who may have contact with the device and/or media.
   - The service provider shall protect the device and/or media from unauthorized access while servicing or storing the device and/or media on behalf of the owner.

c) In cases where a device and/or media is turned over to an external service provider for warranty service or other legitimate purposes, and the machine or media cannot be wiped prior to doing so because of technical malfunction:
   - A legally binding contract must be in place that requires the service provider to protect any information on the device and/or media from unauthorized access. UNH device and/or media owners who do not have such contract in place with their external service providers shall immediately contact their service provider and initiate a deliberate effort to develop and sign such contract as soon as is reasonably practical.
   - The service provider must protect the device and/or media from unauthorized access, and wipe or completely destroy the device and/or media to at minimum the UNH wiping and documentation requirements.

d) Also see USNH Purchasing Surplus Property at [http://www.unh.edu/purchasing/surplus/index.html](http://www.unh.edu/purchasing/surplus/index.html). Please be sure to wipe, or make arrangements to wipe your media before submitting it into the Surplus Property process. Doing so not only helps you remain compliant with the System Access Policy, but it also helps to protect your privacy, as well as privacy of those whose information you manage.

e) The minimum standard for “wiping clean” shall be overwriting the entire media at least three times, writing zeros in at least one of the passes and a random set of characters in at least another of the passes. This minimum standard shall be updated as frequently as necessary to improve protection from evolving threats. The “Secure Erase” Option that is built into certain hard drives also meets the minimum requirement. For additional information and guidance for best practices also see the NIST Special Publication 800-88 and the DoD standard 5220.

f) Commercial, custom, and/or manual methods and tools may be used as long as they meet the above minimum standards, and the method/tool is tested to ensure that it is effective.
g) Where wiping is impossible or impractical, complete physical destruction of media through proven professional services that are guaranteed to eliminate the possibility of reconstructing the data, and that are compatible with environmental regulations shall be an acceptable alternative. Protection of the media from unauthorized access must be ensured until the point of destruction.

h) The CIS Computer Service Center provides a fee-based wiping service. Please contact the Computer Service Center in advance to confirm details and to schedule the service.

i) Owners of devices must consider whether those devices contain institutional data. For example, some of the less obvious devices that have been found to contain restricted and sensitive (see USNH Data Classification Model) data include printers, faxes, copiers, iPods, MP3 players, etc. Those devices must be wiped as well.

j) Personal devices that cannot be wiped with established hard drive wiping mechanisms but be wiped, at minimum, following the wiping instructions provided by the manufacturer.

k) In all cases, wiping of data and destruction of media shall be documented and such records shall be retained for two years by the owner (in cases where the owner performs the wiping) or the service provider who wiped the media.

5.7.1.6 Social Security Number (SSN) is a particularly sensitive data item for all constituents. Whenever the SSN is utilized and/or displayed, the following shall apply to mitigate its exposure to unauthorized access.

5.7.1.6.1 A SSN shall not be sent via e-mail unless encrypted or masked for all but the last four (or fewer) digits of the number.

a) Electronic message are not considered a secure communication mechanism. Messages can be misdirected, resent by mistake or through malicious software infections, and exist for extended periods of time in e-mail accounts, when synchronized to local drives and PDAs, and backed up to long-term storage media. Electronic messages are among the most common causes of data breaches with potentially serious and expensive consequences.

b) USNH institutions are working together to conduct a Request for Proposal for a quality encryption solution or service that will offer a superior option for protecting content in transit and at rest. Outcomes of this RFP will not be available prior to May1. Safe and effective temporary alternatives must be considered.

c) CIS offers file sharing options with enhanced security protection to which clients should migrate protected content from departmental or Public Server Services systems. Restricted and sensitive data should be removed from
storage systems where it is not needed, and when migrating such data to the enhanced security file sharing option provided by CIS, only needed data should be brought into that system.

5.7.1.6.2 Shared electronic and paper reports shall have all but the last four (or fewer) digits of the SSN masked. In the limited cases where SSN is required for regulatory compliance related to employment, payroll processing, provision of benefits, and tax reporting, access to the information shall be limited to those with need to know.

5.7.1.6.3 Paper and electronic documents containing a SSN shall be disposed of in a secure fashion.
   a) When deleting electronic files or e-mail messages with SSNs, also empty the electronic “recycle bin”, “trash can” and/or take other steps to permanently remove the content so it cannot be easily recovered. On some systems this process is also called “purging” or “emptying the trash bin”.
   b) Also see data wiping and media destruction above.
   c) Permanently deleting content from production system must include consideration of where else the content is stored, such as on backup media and printed form, and appropriately deleting or destroying such copies of the content.

5.7.1.6.4 Personal information which links a SSN with a person shall not be publicly displayed.

5.7.1.7 Access to systems and sensitive data from outside the USNH managed environment (for example, from employee homes or during travel) will meet the same level of secure access as is provided in the USNH-managed environment.
   a) See the “Information Technology Best Practices” section of http://cis.unh.edu/itsecurity, and additional specific standards required by your service provider.
   b) When working from off-campus, protect your computer and logged-in sessions from unauthorized access by others. Employ secure connectivity options, such as secure wireless options and VPN, but do so only if your computer is appropriately configured and protected in the first place. Logging into UNH information technology systems with an infected or compromised personal computer or device through a secured connection seriously endangers UNH information technology systems, data and personal privacy.
   c) Secure access starts with a healthy workstation, which requires a current operating system for which the vendor has current security patches. It requires a quality and current malicious software
protection program, at minimum comparable to that of McAfee. The computer should be setup following the best practices followed for administrative systems on the campus (for example the PDNC configuration at UNH that is appropriate for administrative systems). User accounts on the machine need to use strong passwords and follow the System Access Policy for the frequency of changing the password.

d) The computer that is used to access secure institutional systems should not be used by others, especially if the others are likely to log into insecure environments, browse web sites that could have malicious links, and install applications that put the machine at risk. Examples of such applications include chat programs and peer-to-peer file sharing programs.

e) Campus machines are occasionally scanned for vulnerabilities when connected to the campus network. To accomplish the same level of secure access from off campus, alternate methods must be established to check the computer for vulnerabilities.

f) Do not download institutional information to personally owned computers and media, and/or to computers or media that is used by others.

g) Institutional portable devices, such as but not limited to laptop computers that contain restricted data and are carried outside of secure office space must be encrypted.

h) Users shall not log into secure UNH environments that have restricted data (Banner HR) from public equipment, such as kiosk machines at conventions or unsecured wireless services in public hot spots.

5.7.1.8 The Chief Information Officer at each USNH institution will establish standards and interpret this policy to assure that it is implemented in a manner consistent with the technologies at each institution.

5.7.1.9 This policy revision will be effective May 1, 2009.