

NBS Rules of Behavior

October 07, 2009



National Institutes of Health Business System (NBS)

Rules of Behavior



October 2009

All NBS documentation related to security is "Confidential" and will be marked as such. Distribution of NBS security documentation to any individual or organization without a need-to-know is forbidden. Contains sensitive information – Knowing or willful disclosure of sensitive information can result in criminal penalties associated with the Privacy Act, Computer Security Act, and other Federal laws that apply.

NBS Rules of Behavior

October 07, 2009



1. Introduction

Rules of Behavior establish standards that recognize knowledgeable users are the foundation of a successful security plan. These rules clearly define standards of behavior for all NIH personnel who access NBS, including contractors and other federally funded users. Non-compliance of these rules will be enforced through sanctions equal to the level of infraction. As described in the *NIH Enterprise Master IT Security Plan*, sanctions may range from a written or verbal warning, removal of system access for a specific time period, reassignment to other duties, or termination, depending on the severity of the violation. NIH will enforce the use of penalties against any user who willfully violates any NIH or federal system security (and related) policy as appropriate. Users are also responsible for reporting security incidents, or any incidents of suspected fraud, waste, or misuse of NIH systems to Information Security and Awareness Office.

The rules set forth in this document are not to be used in place of existing policy; rather they are intended to further delineate and highlight the specific rules each user must follow while accessing and using NBS. As a supplement, these NBS Rules of Behavior are consistent with the policy, procedures and rules described in the following directives and included in the NIH Security Awareness Training:

The NIH Enterprise Master IT Security Plan, Section 4.1.2 (Rules of Behavior) includes policies regarding accountability, remote access usage, appropriate use of the Internet and email, access controls, password selection, and information management. These policies can also be found online, designated as the NIH Information Technology General Rules of Behavior, at http://irm.cit.nih.gov/nihsecurity/NIH_Enterprise_Master_Security_Plan.doc. The NBS Rules of Behavior map directly to the *NIH Enterprise Master IT Security Plan* Rules of Behavior.

The Department of Health and Human Services (DHHS) *Information Security Program Policy*, *Information Security Program Handbook* and specific Information Resource Management (IRM) policy documents contain computer security guidance on a wide range of topics and describe implementing and administering an information security program that establishes policies, procedures, and responsibilities in the area of computer security within the Department. It is available at http://irm.cit.nih.gov/security/sec_policy.html

NIST Special Publication 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems, gives an overview of system security requirements, as directed by the government, and provides guidance on creating a security plan that describes the controls in place or planned for meeting those requirements.

2. Physical Security

Physical security focuses on protecting and limiting access to the office facilities and the hosting facility for NBS. Office and hosting facilities contain important information assets and it is important that unauthorized persons not have ability to gain access. This is especially crucial due to the sensitive nature of NBS information as well as the fact that access to the system is spread across disparate locations. NBS employers, contractors and users should:

- Keep all badges, access codes, and keys under personal protection.
- Wear your assigned identification security badge at all times while in NIH facilities.
- Ensure your visitors have are escorted at all times.
- Never allow any individual who does not have proper identification access to the office space.
- Stop and question any individual who does not have proper identification, and contact NIH Police Branch (301-496-2387) immediately for assistance to remove an intruder. Seek the support and cooperation of co-workers as appropriate. The following website provides more information in regards to the services provided by the NIH Police Branch: http://ser.ors.od.nih.gov/police_other.htm.
- Maintain control over your NIH provided hardware/software to prevent theft, unauthorized use/disclosure, misuse, denial-of-service, destruction/alteration of data, or violation of Privacy Act restrictions.

3. Computer System Responsibilities

Whereas physical security is concerned with the strength of the building access controls, computer system responsibilities focus on the software and applications. Users must address these responsibilities when using NBS to prevent possible threats to the system. For example, installing computer programs of unknown origin can introduce security vulnerabilities due to questionable coding and therefore should be limited. Documents must be properly disposed of to ensure valuable information does not remain for others to possibly exploit. The misuse of NBS and the weakening of its security controls could compromise the integrity of NBS data and prevent NBS from doing its job to the detriment of the NIH mission. NBS employers, contractors and users shall abide by the following requirements:

- Do not make copies of system configuration files for your own use, unauthorized use, or to provide to others for unauthorized use.
- Do not, without specific authorization, read, alter, or delete any other person's computer files or e-mail, even if the operating system of the computer allows you to do so.
- Unless otherwise expressly authorized, do not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system.
- No user, software developer, or Web developer should write or put into production any computer code, program, or script that is considered to be a "Trojan Horse" (applications

NBS Rules of Behavior

October 07, 2009



that attempt to circumvent any security measures) or any other malicious software that would cause harm to the system including viruses, worms, or any “back door” means of accessing the system or applications.

- Any user found to introduce malicious software, coding, programs, or scripts, is subject to prosecution under local, state, and federal law and is subject to local department policies, which enforce disciplinary action up to, and including dismissal.
- Users should never attempt to circumvent any security measures for software applications. This includes the hard coding of passwords.
- Use only NBS, software, and data for which you have an expressed authorization and use them for authorized purposes only.
- Protect confidential and/or sensitive information from disclosure.
- Perform backups of system data as appropriate. Refer to the CIT disaster recovery plan for detailed information on backup procedures.
- Destroy hard copies of highly sensitive information, especially Privacy Act data or financial information, by pulping or shredding.
- Highly sensitive information stored on removable media should be entirely erased, or the disks destroyed. When disposing of, or transferring a computer system, erase all files from the hard drive by using a wipe out utility, or destroy the disk if necessary according to the NIH Records Management Guidelines. Please refer to the following URL for the current NIH Sanitization policy: <http://irm.cit.nih.gov/security/sanitization.html>.

4. Access Control

Access control procedures provide direction for allocating the appropriate amount of access to users to allow them to utilize only the information and applications necessary for their jobs. Users can also help prevent information from being unnecessarily disclosed by adhering to the following procedures:

- Grant access to NBS and data only to those who have an official need to know.
- Never share or compromise your password.
- Select a password in accordance with NIH password policy requirements. The current policy is located at http://irm.cit.nih.gov/nihsecurity/pwd_policy.doc
- Do not share passwords with anyone; make alternative provisions for access to information during a personal absence to avoid sharing passwords.
- Users are required to log-off the NBS when it is not in use.
- Include the following disclaimer on the fax cover sheet when sending faxes:

****WARNING****

NBS Rules of Behavior

October 07, 2009



The attached information may be confidential. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.

- NBS will have the following warning banner upon system login and will be applicable to all those whom access the system:

****WARNING****

This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

5. Unofficial Use of Government Equipment and Services

Government assets are the property of the United States Government and should be used for work related functions.

- Do not utilize government resources for commercial activity, or any venture related to personal profit or gain.
- Do not utilize government resources for behaviors that are unethical or unacceptable for the work environment, such as improper usage of funds or purchasing equipment without proper approval.
- For additional guidance on acceptable use of Government assets, please review the Limited Authorized Personal Use of NIH Information Technology (IT) Resources policy at <http://www3.od.nih.gov/oma/manualchapters/management/2806/>

NBS Rules of Behavior

October 07, 2009



NBS Rules of Behavior User Agreement

I acknowledge receipt of and understand my responsibilities outlined in this document as well as those outlined in the NIH Master Security Plan. I will comply with the Rules of Behavior as outlined.

Signature of User

Date

Print Name

Organization, Office or Company

Signature of Supervisor

Date

Print Name

Organization, Office or Company