U.S. Nuclear Regulatory Commission
Agency-wide Rules of Behavior for Authorized Computer Use

~~May 19, 2009~~

Version 1.1, April 27, 2011

1. Introduction

Federal directives require agencies to establish rules of behavior for individual users to govern the secure use of information technology (IT) computing resources. The U.S. Nuclear Regulatory Commission (NRC) Agency-wide Rules of Behavior for Authorized Computer Use shall be referred to as the "rules of behavior". This document specifies user level rules for the secure use of all computing resources used to process or store sensitive NRC information. Sensitive information is any information where a compromise of the confidentiality, integrity, or availability of the information would cause adverse effect on NRC operations, NRC assets, or any individuals.

User violation of these rules will be reported to the user's management and to the Computer Security Office (CSO). Non-compliance may subject the user to disciplinary action, as well as penalties and sanctions, including verbal or written warning, removal of system access privileges, reassignment to other duties, criminal or civil prosecution, and/or removal from Federal service, depending on the severity of the violation.

2. Scope

The rules of behavior apply to all NRC employees and support contractors at their primary workplace and at any alternative workplaces (e.g., teleworking from home or from a satellite site) and to users on official travel. This document refers to these persons as nonpublic users. The document establishes agency level rules of behavior as required by OMB Circular A-130, and supports requirements from other related policies as identified in Appendix A, "References."

Users must acknowledge their responsibilities when using NRC IT resources in accordance with these rules by agreeing to the rules of behavior acknowledgement statement at the end of the annual ~~computer~~cyber security awareness course. The acknowledgement statement can also be viewed at the following URL:

http://www.internal.nrc.gov/CSO/documents/ROB_Ack.pdf

Individual systems may require separate acknowledgement of additional rules depending on the nature of the system and of the information processed by that system. In such cases, users are required to acknowledge that they will abide by system-specific rules in addition to these universal NRC rules of behavior as a condition of gaining and retaining access to the system.

3. Rules of Behavior for Nonpublic Users

The following rules apply to all NRC nonpublic users of NRC computing resources. These rules are based on and are consistent with policy and procedures in NRC MD 2.7, "Personal Use of Information Technology," and MD 12.5, "NRC Automated Information Security Program".

3.1   System Access and Use

Preventing unauthorized access to NRC IT systems and information requires the full cooperation of all users for effective and successful security. Users must be aware of their responsibilities for maintaining effective access controls, particularly regarding the use of identification and authentication information and strict adherence with the permissions granted to them.

The following rules of behavior are relevant to NRC system access and use. Users shall:

- Use Government-owned or Government-leased computing resources for work-related purposes only except as allowed by MD 2.3, "Telecommunications"; MD 2.7; and MD 12.5. No other unofficial use is authorized.

- Adhere to all Federal laws, NRC security policies, standards, and directives.

- Be responsible for all actions performed using his or her user account, and shall not allow others access once he or she has logged on to any system.

- Use only Designated Approving Authority (DAA) approved business solutions when traveling outside of the country.

- Access and use only information or systems for which he or she has official authorization.

- Follow established procedures for accessing information, including the use of user identification (ID), ~~passwords,~~authentication information (e.g., personal identification numbers, passwords), and other physical and logical safeguards.

- Follow established procedures for requesting and disseminating information.

- Access only those files, directories, and applications for which the user has been granted access authorization in accordance with their job function and agency policy.

- Ensure all sensitive information is protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This protection may be accomplished by screens, hoods, or positioning the equipment (monitors or printers) so that they face away from doorways, windows, or open areas.

- Terminate sessions or employ a session-locking mechanism that requires user re-authentication to regain session access before leaving equipment unattended for even a short duration.

- Log off of all equipment and sessions when leaving equipment for the day unless a specific need has been established to remain logged in and that need has been approved by the user's supervisor and the system owner.

Users shall not:

- Use NRC computing resources to conduct or support a personal business.

- Place unauthorized software onto an NRC computing resource.

- Install peer-to-peer (P2P) software on NRC computers without explicit written approval of the DAA.

- Use any computing resource to process NRC information unless it has been

approvedauthorized by the system ownerDAA.

- Connect a computing resource to any system, including infrastructure systems, without the permission of the system ownerDAA authorization.

- Divulge access information (e.g., login procedures, lists of user accounts) for a computing resource to anyone who does not have a need to know the information as determined by NRC management.

- Make unauthorized copies of security or configuration information (e.g., the /etc/passwd file) on a computing resource for unauthorized personal use nor divulge this information to anyone who does not have a need to know the information as determined by NRC management.

- Leave an open login session unattended. The user shall either log out or use a password-enabled screen saver that requires user authentication to protect against unauthorized use.

- Bypass system controls or access data for any reason other than official duties.

3.2   Passwords, Digital Certificates, and Other Electronic Access Control Measures

Identification is the process by which a person, device, or program is differentiated from all others. User identification is commonly provided in the form of User-IDs, but is also provided using other methods, such as digital certificates.

Authentication is the process by which user identification is verified. Authentication can be performed using passwords, cryptographic keys, digital certificates, biometrics, access cards, tokens, or other methods.

To protect access to computing resources users shall:

- Protect passwords (including access numbers)Protect authentication information at a level commensurate with the sensitivity level or classification level and classification category of the information to which the authentication allows access.

- Protect authentication information from disclosure and shall not record them in writing or in electronic form except when they are protected against unauthorized access at a level comparable to the sensitivity of the information that may be accessed using the passwordauthentication information.

- Promptly change a password authentication information whenever compromise is known or suspected.

- Construct passwords that meet the minimum length requirements for the system or device being accessed and include upper and lower case letters, numbers, and special characters as mandated by OMB common security configuration requirements.

- Choose passwords that do not contain information associated with the user, such as names, car registration or tag numbers, and telephone numbers.

- Select passwords that do not and use words (spelled forwards or backwards) found in a dictionary, and that are not based on a single word (e.g., "Pa$$wOrd").

- ~~Not attempt to bypass or circumvent access controls to a computing resource.~~

- ~~Protect passwords by not sharing them with any other person, including the user's supervisor or Help Desk worker.~~

- ~~Select and use a~~ unique ~~password~~authentication information for access to each computing resource or group of computing resources subject to applicable ~~password~~authentication information restrictions.

- Notify their IT coordinator or contact the NRC help desk when experiencing difficulties with a user account or ~~password(s).~~authentication information.

- Report any suspected or known authentication information (e.g., password) compromise to the system ISSO and to the NRC Computer Security Incident Response Team (CSIRT) at 301-415-6666 or CS_IRT@nrc.gov.

- Construct and maintain passwords in accordance with CSO-STD-0001, NRC Strong Password Standard.

- Users shall not:

- Allow anyone to know or use their identification and authentication information to access an NRC IT system. Except in the case of initial use authentication information or authentication information reset at the user request, only the user shall have knowledge of the authentication information.

- Allow anyone else to use their computer while they are logged into the system. Users are responsible for any activity initiated while they are logged into the system

- Attempt to bypass or circumvent access controls to a computing resource

- Store authentication information on-line (including password saving features of operating systems and applications), except in the case of initial use and reset authentication information or where a DAA-approved secure authentication information capability has been provided

- Use the same authentication information for NRC system access and non-NRC purposes

3.3   Electronic Data Protection

The user is responsible for protecting the confidentiality, integrity, and availability of NRC information and files, and storage, disposal, mailing, and electronic transmission of sensitive information shall be in accordance with Federal and NRC policies and directives. For a complete list of Federal and NRC policies and directives related to this policy, please refer to Appendix A - References. Users shall not create or maintain a Privacy Act system of records (e.g., files of individuals retrievable by name and/or personal identifier) on an NRC system without approval of the NRC Senior Agency Official for Privacy. Users shall protect ~~Office of Investigations (OI) and Office of Inspector General (OIG) investigation-related~~sensitive unclassified non-safeguards information (SUNSI) documents ~~according to the~~in accordance with guidance located at http://www.internal.nrc.gov/sunsi/~~investigation~~index.html.

3.3.1   Electronic Personally Identifiable Information

For the purpose of these rules of behavior Personally Identifiable Information (PII) is information that can be used to uniquely and reliably identify or contact a person or which can be traced

Formatted: Normal

Field Code Changed

back to a specific individual. For example, a person's name in combination with relatives' names, postal address, home e-mail address, home or cellular telephone number, personal characteristics, social security number, date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily traceable. To protect PII, users shall:

- Use ~~password~~authentication information protection and where possible, automatically lock out after ~~30~~15 minutes (or less) of user inactivity all mobile computing resources on which PII is stored.

- Identify files, extracts or outputs he or she creates or has created that contain PII and delete those that have no business purpose.

Users shall not:

- Remove electronic PII from NRC-controlled space unless all PII is encrypted using a cryptographic method approved by an NRC Chief Information Security Officer (CISO). SecureZip has been installed on NRC desktops and is a CISO-approved cryptographic method.

- Use personally owned computing resources for processing or storing PII of individuals pertaining to NRC official business other than themselves, except as formally (i.e., in writing as an official record) approved by the DAAs.

- E-mail or otherwise transmit PII outside of the NRC's infrastructure, except when necessary to conduct agency business. E-mailing PII within the NRC LAN or wide-area network is acceptable, including to and from BlackBerry handheld devices that interact within the NRC's e-mail system.

~~It~~NRC considers personal identity to be distinct from an individual's professional identity; that is, an employee's name, title, work telephone number, official work location, and work email address are not treated by NRC as PII. Additionally, at NRC it is not necessary to remove home addresses, home ~~telephone~~phone numbers, ~~and personal e-mail~~or home email addresses from adjudicatory filings~~,~~ (generally refer to domestic licensing proceedings and related orders under 10 CFR Part 2), documents associated with agency ~~rulemaking~~rulemakings, and correspondence received from the public on regulatory matters~~ since information in these types of agency correspondence (i.e., to and from the agency) are not treated as PII. ~~.

3.4   Use of Government Office Equipment

Users shall limit their personal use of NRC office equipment in accordance with NRC MD 2.7.

3.5   Use of Software

- Users shall abide by Executive Order 13103 and U.S. copyright laws when using NRC systems, and shall not acquire, install, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.

3.6   Internet and E-mail Use

Users of the NRC Internet and electronic mail services and resources shall:

- Limit personal use of the Internet and e-mail in accordance with NRC MD 2.7.

- Understand that Internet and e-mail use may be monitored, and by signing

these rules of behavior consent to such monitoring.

- Acknowledge that any e-mail on a Government e-mail system is the property of the Government and may become an official record.

- Not use Internet and electronic mail for fraudulent or harassing messages or for sexual remarks or the downloading of illegal or inappropriate materials (e.g., pornography). Additionally, users shall not send or retain any such material on any Government system. Inappropriate usage includes providing illegal copies of software to others through file-sharing services, and making threats to another person via e-mail.

3.7   Teleworking

When authorized to telework from home or from other alternate workplaces users shall:

- Use only NRC-approved technologies for remote access to the NRC network.

- Follow security practices that are the same as or equivalent to those required at his or her primary workplace when teleworking from an alternate workplace.

- Physically protect all computing resources when they are not in use.

- Protect sensitive data at his or her alternate workplace, including proper disposal of sensitive information (e.g., shredding using approved shredders).

3.8   Protection of Computing Resources

Users of NRC computing resources used to process NRC information or to connect to NRC systems shall:

- Implement security controls as directed by NRC policy and procedures.

- Use only NRC furnished computing resources (or approved personally owned equipment) to access NRC systems and information.

- Maintain physical control of NRC computing resources at all times, and take all necessary precautions for their protection against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.

- Keep operating system, antivirus, application, and firewall software on the computing resources up to date.

- Use only NRC-authorized Internet connections that conform to NRC security and communications standards.

Users shall not:

- Make any changes to an NRC computing resource's system configuration unless directed to do so by an authorized NRC system administrator.
- Program a computing resource with NRC sign-on sequences, NRC passwords or other authentication information, or NRC access phone numbers.
- Use wireless solutions and configurations that are not specifically approved by the NRC DAA, and shall not process, store, or transmit sensitive information on wireless devices unless encrypted using CSO-approved encryption methods.

3.9   Information Technology Incident Reporting

Despite advances in automated intrusion detection systems, computer users are frequently the first to detect intrusions that occur, and must be vigilant for questionable activities or behavior that may indicate that a computer security incident is in progress. Users will report actual and suspected incidents immediately to the NRC Computer Security Incident Response Team (CSIRT). Examples of incidents include:

- Suspicious e-mail activity, including SPAM, phishing, e-mail originating from unknown sources, and volume emailing.
- Receipt of obscene, racist, profane, libelous, or offensive e-mail.
- Unusual phone calls (e.g., soliciting personal or IT system information).
- Automatic installation of unknown software.
- Requests for user identification and passwordauthentication information.
- Computer use in NRC facilities by unknown or unidentified individuals.
- Losses or compromises of PII.

Users must report any actual or potential incidents immediately to the CSIRT by telephone at 301-415-6666 or by e-mail at CS_IRT@nrc.gov. Additionally, lost, damaged, or stolen computing resources (e.g., desktop computer, cell phone, BlackBerry, laptop, thumb drive) either actual or suspected, shall be reported immediately to the CSIRT and NRC Office of Administration, Division of Facilities and Security, by telephone at 301-415-2056.

Field Code Changed

3.10   User Accountability

Unauthorized use of a user account or a computing resource is a violation of Section 1030, Title 18, of the United States Code; constitutes theft; and is punishable by law. Users will be held accountable for their access and use of NRC computing resources.   Users shall:

- Have no expectation of privacy while using any NRC computing resource including the NRC Internet, Intranet, or e-mail services.
- Complete NRC-mandated security awareness courses, briefings, and updates and all mandated training commensurate with user IT security responsibilities at the required frequency and before accessing NRC systems.
- Read and understand warning banners and end-user licensing agreements.

4. Rules of Behavior for Privileged Users

The rules of behavior in this section apply to all privileged users with either limited or unlimited

privileged access to ~~U.S. Nuclear Regulatory Commission (~~NRC~~)~~ systems. Privileged users are usually those users with one or more of the following functions:

- System administrators
- Computer operators
- System engineers (i.e., those with control of the operating system or specific application software)
- Network administrators
- Database administrators
- Those who control user ~~passwords~~authentication information and access levels

Privileged users must make an effort to notice the threats to and vulnerabilities of information systems. They must make these known to management, and work to develop effective countermeasures. Privileged users shall do the following:

- Respond to security alerts and requests by NRC IT security managers and the CSO.

- Protect the supervisor or root-level ~~password and~~ authentication information at the highest level demanded by the sensitivity of the system.

- Use special access privileges only when they are needed to carry out a specific system function.

- Use a non-privileged (i.e., general user) account whenever administrative privileges are not required (e.g., email, web browsing).

- Never use special privileges for personal business, gain, or entertainment.

- Use precautionary procedures to protect a privileged account from fraudulent use.

- Use security measures to ensure integrity, confidentiality, and availability of information contained in the systems.

- Watch for signs of inappropriate or illegal (e.g., hacker) activities or other attempts at unauthorized access and report them to the CSIRT upon discovery.

- Assist with recovery activities and take appropriate action to reduce damage from security violations.

- Alert the appropriate personnel when a system goes down or experiences problems.

- Ensure that systems and data are properly backed up and that the

configuration is adequately documented for recovery purposes.

- Give a general user or other privileged user access only to those systems and information for which he or she requires access to perform official duties.

- Read, understand, and enforce the system security controls as defined in the system security plan.

APPENDIX A: REFERENCES

The following references will aid the user in understanding the rules of behavior:

- Appendix III "Security of Federal Automated Information Resources," to OMB Circular A-130,"Management of Federal Information Resources"

- National Institute of Standards and Technology (NIST) Federal Information Processing ~~Standard~~Standards

- NIST Special Publications

- ~~NRC MD 2.7~~

- ~~NRC MD Volume 12, "Security"~~

- NRC Management Directive (MD) 2.7, ""Personal Use of Information Technology"

- NRC MD and Handbook 3.2, "Privacy Act"

- NRC MD Volume 12, "Security"

- NRC Privacy Act Web page http://www.internal.nrc.gov/ois/divisions/irsd/privacy/index.html

- NRC PII project home page http://www.internal.nrc.gov/PII/index.html

- NRC Sensitive Unclassified Non-Safeguards Information (SUNSI) Program ~~http://www.internal.nrc.gov/ois/divisions/irsd/sunsi/index.html~~http://www.internal.nrc.gov/ois/divisions/irsd/sunsi/index.html

- The Federal Information Security Management Act of 2002

- Public Law 99-474 (Title 18, United States Code), section 1030

- Executive Order 13103, "Computer Software Piracy"

- OMB memoranda

  - M-05-08, "Designation of Senior Agency Officials for Privacy"

  - M-06-15, "Safeguarding Personally Identifiable Information"

  - M-06-16, "Protection of Sensitive Agency Information"

  - M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"

  - M-06-20, "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

  - M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

  - M-07-18, "Ensuring New Acquisitions Include Common Security Configurations"

  - M-08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)"

  - M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies"

  - M-10-23, "Guidance for Agency user of Third-Party Websites and Applications"

| Field Code Changed |
| Field Code Changed |

- M-11-02, "Sharing Data While Protecting Privacy"

- M-11-06, "WikiLeaks - Mishandling of Classified Information"

- M-11-08, "Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems"

- M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"

- NRC Yellow Announcements

  - YA-06-0039, "Safeguarding Personal Privacy Information"

  - YA-06-0065, "Use of E-Mail and Other Information Technology at NRC"

  - YA-06-0069, "Protection of Personally Identifiable Information"

  - YA-06-0101, "Policy Reminder on Personal Use of Information Technology and Consequences for Misuse"

  - YA-07-0071, "Privacy at the NRC"

  - YA-07-0106, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

  - YA-07-0114, "Clarification of Waiver Policy for Personally Identifiable Information and Issues Pertaining to Sensitive Unclassified Non-Safeguards Information"

  - YA-08-0006, "NRC Policy and Procedures for Copying, Scanning, Printing, and Faxing Safeguards and/or Classified Information"

  - YA-08-0021, "Policy Revision: Policy Prohibiting the Use of P2P Software, and Its Impact on Processing Sensitive Unclassified Non-Safeguards Information on NRC Information Technology Systems, Mobile Devices, and Home Computers"

  - YA-08-0063, "Information Security and Records Management Requirements When Using Information Sharing and Learning Technologies Such as Sharepoint and Tomoye"

  - YA-08-0092, "Information Technology Implementation Policy—Computer Security Information Protection Policy"

  - YA-08-0093, "Information Technology Implementation Policy—Updated Computer Security Incident Response and Personally Identifiable Information Incident Response"

  - YA-08-0157, "Information Technology Security Policy—Encryption of Data at Rest"

  - YA-09-0035, "Information Technology Security Policy—Laptop Security Policy"

  - YA-11-0038, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Homeland Security Presidential Directive 12 for Access to U.S. Nuclear Regulatory Commission Facilities and Information Systems"

- NRC Policy Memoranda

  - "Protection of Personally Identifiable Information" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML062010292)

- "U.S. Nuclear Regulatory Commission Personally Identifiable Information Breach Notification Policy" (ADAMS Accession No. ML083650337)

- IT security policies and guidance located on CSO Web pages

  - http://www.internal.nrc.gov/CSO/policies.html
  - http://www.internal.nrc.gov/CSO/guidelines.html
  - http://www.internal.nrc.gov/CSO/trainingprocedures.html
  - http://www.internal.nrc.gov/CSO/Site-Indexprocesses.html
  - http://www.internal.nrc.gov/CSO/security_templates.html
  - http://www.internal.nrc.gov/CSO/standards.html
  - http://www.internal.nrc.gov/CSO/training.html
  - http://www.internal.nrc.gov/CSO/Site-Index.html

| Field Code Changed |
| Field Code Changed |
| Field Code Changed |
| Field Code Changed |

APPENDIX B: GLOSSARY

Computing Resource	Computers and IT resources, including desktop and laptop computers, networks, facilities, printers, scanners, faxes, PEDs, cell phones, electronic media, printouts, and any other IT used to store or process information.
Designated Approving Authority (DAA)	The individual(s) responsible for approving IT implementations for operation.
Electronic Media	Different types of data storage options. Electronic storage options change very quickly and include, but are not limited to, the following: • hard drives (i.e., both internal and external) • removable drives (e.g., Zip disks) • compact disks (CDs) • digital video disks (DVDs) • thumb drives • flash memory • floppy disks • magnetic tapes
General User	A person with nonprivileged access to a computing resource. A user may use and access his or her own information and the information available to all users on the computing resource (e.g., commands like passwd, pwd), but the user is restricted from the use of and access to the privileged-level information on the computing resource. A user cannot alter or bypass the security controls on a computing resource.
Information	Datasets, scripts, programs, applications, utilities, files, directories, file systems, databases, and any other data maintained in any medium on a computing resource.
Non-Privileged Account	A user account with either limited access privileges to a computing resource, such as those assigned to a general user. A non privileged account cannot alter or bypass some or all of the security controls on a computing resource.
Nonpublic User	NRC employees and support contractors at their primary workplace and at any alternative workplaces (e.g., teleworking from home or from a satellite site) and users on official travel.
Portable Electronic Devices	PEDs include personal digital assistants (PDAs) (e.g., Palm Pilots), cell phones, text messaging systems (e.g., BlackBerry), universal serial bus (USB) flash memory (e.g., thumb drives), external drives, and plug-in and

Formatted Table

	wireless peripherals.
Portable Mass Storage Device	Include flash memory devices (e.g., FlashDrive, PenDrive, KeyDrive, ThumbDrive, JumpDrive), compact flash, solid-state USB hard drives (e.g., Sony Micro Vault), and Zip disks.
Privileged User	A person with either limited or unlimited privileged access to a computing resource, such as a system administrator or information system security officer. A privileged user is also a user and may therefore use and access his or her own information and the information available to all users on the computing resource. However, a privileged user, unlike a general user, may also use and access privileged-level information on all or part of the computing resource. A privileged user may alter or bypass some or all of the security controls on a computing resource.
Sensitive Information	Any information that is not releasable to the public, including SUNSI, Safeguards Information, and classified information.
User	A general user, nonpublic user, or a privileged user of NRC computing resources.
User Account	Refers to the unique character string used in a computing resource to identify a user. A user account (e.g., an account, a login, a login ID, a login name, a member ID, a user ID, a username) is used by a user with a password or other authentication information to gain access to a computing resource and to maintain the security of the information on a computing resource.