

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

Version 1.34, July 4, 2015 ~~13, 2017~~

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 as a security incident to the user's management, to the Computer Security Incident Response Team (CSIRT), and to the Chief Information Security Officer. 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, contractors, and other users that authenticate to NRC systems and who process, store, or produce classified national security information, Safeguards Information (SGI), sensitive unclassified non-safeguards information (SUNSI), or non-sensitive information using IT systems or IT facilities that are under the security jurisdiction of the NRC 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. SUNSI includes Personally Identifiable Information (PII). This document refers to these persons as non-public users. The document establishes agency level rules of behavior as required by the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources as a Strategic Resource," 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 security awareness course. The acknowledgement statement can also be viewed at the following uniform resource locator (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 Non-public Users

The following rules apply to all NRC non-public users of NRC computing resources. These rules are based on and are consistent with policy and procedures in NRC Management Directive (MD) 2.7, "Personal Use of Information Technology," and MD 12.5, "NRC ~~Cyber Security~~Cybersecurity 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.
- Understand that NRC is not responsible for recovering and/or providing to the user any personal information stored on government equipment.
- Adhere to all Federal laws, NRC security policies, standards, and directives.
- Be responsible for all actions performed and activities initiated using his or her user account.
- Use only ~~Designated Approving Authority (DAA)~~NRC Authorizing Official (AO) 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), authentication information (e.g., personal identification numbers, passwords, digital certificates), 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 the user's 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.

ML15056A494

- 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:

- Allow anyone else to use their computer while they are logged into the system except where a system administrator logs into the system to assist the user with a problem. In that case, the administrator's actions are associated with the administrator's identification and authentication information even though the user has permitted access to his or her account.
- 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 [DAAAO](#).
- Use any computing resource to process NRC information unless it has been authorized by the [DAAAO](#).
- Connect a computing resource (e.g., cellular phone, USB drive) to any system, including infrastructure systems, without [DAAAO](#) 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 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 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.

ML15056A494

- Promptly change authentication information whenever compromise is known or suspected.
- Select and use unique authentication information for access to each computing resource or group of computing resources subject to applicable authentication information restrictions.
- Notify their IT coordinator or contact the NRC help desk when experiencing difficulties with a user account or authentication information.
- Report any suspected or known authentication information (e.g., password, digital certificate) 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.
- Attempt to bypass or circumvent access controls to a computing resource.
- Store authentication information in writing or 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~~an AO-approved secure authentication information capability has been provided that protects the authentication information from unauthorized access at a level comparable to the sensitivity of the information that may be accessed using the authentication information.
- 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. 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 SUNSI ~~documents~~electronic information in accordance with ~~guidance located at~~ <http://www.internal.nrc.gov/sunsi/index.html>. MD 12.5.

3.3.1 Electronic Personally Identifiable Information

For the purpose of these rules of behavior, PII is information that can be used to uniquely and reliably identify or contact a person or which can be traced back to a specific individual. For example, a person's name in combination with relatives' names, postal address, home electronic mail (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. The Privacy Act only protects PII that is part of a Privacy Act system of records. To protect PII, users shall:

- Ensure that PII retrieved by an individual's name or other personal identifier is maintained in an authorized Privacy Act system of records for which a system notice has been published in the Federal Register.
- Use authentication information protection and where possible, automatically lock out after 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 current business purpose.
- Disseminate, PII only to those NRC employees who have a "need to know" the information to perform their official duties, not "want to know."
- Maintain PII in a manner that will ensure no inadvertent or unauthorized disclosures:
 - Do not leave in open view of others;
 - Use an opaque envelope when transmitting through the mail;
 - Secure paper records in a locked file drawer and electronic records in a password protected or restricted access file; and
 - Do not place or store PII on a shared network drive unless access controls are applied.
- Ensure disposition complies with NRC records disposition schedules.
- Dispose of PII using sensitive waste disposal methods.

Users shall not:

- Remove electronic NRC sensitive data (including PII) from NRC controlled spaces unless it is appropriately encrypted using an NRC-approved cryptographic method. ~~SecureZip and MXI Stealth thumb drives are two examples of approved methods for encrypting and storing electronic NRC sensitive data.~~
- 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 DAAAsAO.
- 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

ML15056A494

LAN or wide-area network is acceptable, including to and from BlackBerry handheld devices that interact within the NRC's e-mail system.

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 e-mail address are not treated by NRC as PII. Additionally, at NRC it is not necessary to remove home addresses, home phone numbers, or home e-mail addresses from adjudicatory filings (generally refer to domestic licensing proceedings and related orders under 10 CFR Part 2), documents associated with agency rulemakings, and correspondence received from the public on regulatory matters.

Formatted: Space Before: 12 pt

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, Messaging, Telephones, Collaboration Tools, Conferencing, Video, and E-mail Use

Users of the NRC Internet, Messaging, Telephones, Collaboration Tools, Conferencing, Video, and e-mail services and resources shall:

- Limit personal use of the Internet and e-mail in accordance with NRC MD 2.7.
- Unless using a system that has been specifically authorized for information at a confidentiality level higher than moderate, understand that information with a confidentiality sensitivity higher than moderate may not be stored, transmitted, or processed by these capabilities.
- 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 information on a Government e-mail system is the property of the Government and may become an official record.
- Copy their official agency e-mail address on any agency business conducted via personal e-mail account or forward a complete copy of said e-mail with 20 days of creation, as may be deemed necessary if the NRC-Approved e-mail system is unavailable.

Users of the NRC Internet, Messaging, Telephones, Collaboration Tools, Conferencing, Video, and e-mail services and resources shall not:

Formatted: Don't keep with next

- Automatically forward NRC e-mail or other messaging to personal email accounts.
- Send SUNSI to personal email accounts.

ML15056A494

- Use [Internet and e-mail](#) [these capabilities](#) for fraudulent or harassing messages or for sexual remarks or the downloading of illegal or inappropriate materials (e.g., pornography).
- Send or retain any such [inappropriate](#) 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](#) [government services](#).

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.
- Protect, physically, 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 Office of Administration [ADM]) approved shredders).

3.8 Social Media

Whether one is using social media for participation as an Authorized NRC Representative, participation while on official duty, or creation of an official NRC-sponsored social media site or account or otherwise using NRC assets, users shall:

- Act in accordance with [NRC ethical conduct requirements](#).
- Maintain a clear and distinct separation between personal opinion and official NRC information. If a personal profile identifies an individual as working for the NRC, or if an NRC employee has a public-facing position such that the general public would know the individual's NRC affiliation, the NRC employee should ensure that his or her profile and related content (even if they are of a personal and not an official nature) are consistent with how he or she wishes to present himself or herself as an NRC professional, are appropriate with the public trust associated with his or her position, and conform to existing standards (e.g., 5 CFR Part 2635).
- Notify the Office of Public Affairs or an employee designated as an Authorized NRC Representative when aware of inappropriate, misleading, or inaccurate information about the NRC while engaged in social media activities.
- Ensure appropriate records are maintained in accordance with MD 3.53, "NRC Records and Document Management Program" for documentary materials created, received, or accessed when using social media.

Users of social media shall not:

- Engage in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.

ML15056A494

- Endorse, oppose, or contribute to any partisan parties, candidates, or groups.
- Post a rebuttal to the incorrect information when aware of inappropriate, misleading, or inaccurate information about the NRC while engaged in social media activities.

3.8.1 Authorized and NRC Sponsored Social Media Representation

When a user is an Authorized NRC Representative or is creating an official NRC-sponsored social media site or account, the user shall:

- Initiate and maintain profiles necessary to fulfill their designated representation responsibilities, such as registering for a forum in order to post information, according to their office's social media guidance.

When establishing accounts/profiles for authorized and NRC sponsored social media representation:

- Ensure the profile complies with NRC computer security policy, standards, and guidance.
- Ensure the user's username is not an NRC account username (e.g., the user's NRC network identifier), should not reflect personal information about the user, and must be approved by the office director or designee.
- Ensure the profile information, such as user's biography, is approved by the user's office director or designee and that it reflects NRC-relevant information that is not sensitive.
- Ensure the profile is linked to the user's NRC e-mail account (John.Doe@nrc.gov) and not to a personal account.
- Ensure the authorized NRC accounts/profiles are restricted to NRC employee work and office-related information only, and no personal information, including personally identifiable information (PII), is included.
- Ensure the authorized NRC profile displays only images approved by the user's office director or designee.

3.9 Microphones

Users of microphones shall:

- Physically disable or disconnect them when not in use. This can be accomplished by physically disconnecting the cable from the computer. Where the microphone is built into the device, the microphone must be turned off via a physical switch, or if a physical switch does not exist, using the keyboard microphone off button.
- Ensure that the area that might be captured by the microphone does not include discussions of any non-public information not pertinent to the conversation.
- Only be used for SUNSI information when participants are in an NRC facility or at an authorized telework location.

ML15056A494

Users shall not:

- Use microphones where SGI information with a confidentiality sensitivity above moderate, SGI, or classified information is present or being discussed unless a specific authorization for such use is provided by the NRC DAAAQ.

3.10 Cameras

Users of cameras shall:

- Physically disable or disconnect them when not in use. This can be accomplished by physically disconnecting the cable from the computer, or blocking the camera lens with a hood or physical strip.
- Ensure that the area that might be captured by the camera does not contain any non-public information not pertinent to the conversation.
- Only be used for SUNSI information when participants are in an NRC facility or at an authorized telework location.

Users shall not:

- Use cameras where SGI information with a confidentiality sensitivity above moderate, SGI, or classified information is present unless a specific authorization for such use is provided by the NRC DAAAQ.

3.11 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 (please see the MD 12 series).
- Use only NRC furnished computing resources that process, store, or transmit information (or approved personally owned equipment using an AO authorized implementation) to access NRC systems and information. Passive equipment, such as a monitor, do not have to be approved.
- 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 in accordance with NRC approved versions.
- 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.

ML15056A494

- Program a computing resource with NRC sign-on sequences, NRC passwords or other authentication information, or NRC access phone numbers. The NRC password wallet does not violate this as the solution has been authorized by the AO, and the user must authenticate to the password wallet using an NRC approved authentication method.
- Use wireless solutions and configurations that are not specifically approved by the NRC DAAAQO.
- Process, store, or transmit sensitive information on wireless devices unless encrypted using CSOCISO-approved encryption methods.

3.12 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 address suspicious e-mail activity, including SPAM, phishing, e-mail originating from unknown sources, and volume e-mailing, by deleting the e-mail without opening the e-mail or its attachments and without clicking on any links within the e-mail and then emptying the e-mail trash folder.

Users will report actual and suspected incidents immediately (within one hour) to the NRC CSIRT. Examples of incidents include:

- E-mailMessages that warrantswarrant attention beyond deletion.
- Receipt of obscene, racist, profane, libelous, or offensive e-mailmessages.
- Unusual phone calls (e.g., soliciting personal or IT system information).
- Automatic installation of unknown software.
- Requests for user identification and authentication information.
- Computer use in NRC facilities by unknown or unidentified individuals.
- Losses or compromises of PII.

Reporting of any actual or potential situations involving the improper handling or storage (no IT equipment/system involved) of SUNSI, SGI, or classified information must be reported immediately (within one hour) to the Office of Administration (ADM), Division of Facilities and Security (DFS) by either (1) selecting the "Report a Security Incident" button located on the NRC internal web page (and select physical security incident), (2) contacting the NRC Security Incident Hotline (301) 415-6666, Option 1, (3) filling out and submitting an NRC form 183; or (4) contacting the DFS duty officer through the Central Alarm Station: 301-415-2056 or 301-415-2000.

Any actual or potential release of SUNSI, SGI, or classified information where IT equipment/system is involved must be reported immediately (within one hour) to the Computer Security Incident Response Team (CSIRT) at CSIRT: CS_IRT@nrc.gov, or 301-415-6666, Option 2.

3.13 User Accountability

Unauthorized use of a user account or a computing resource can result in criminal penalties under Section 1030, Title 18, of the United States Code. 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~~ and messaging 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 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 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 ~~Computer Security Office (CSO), CIO and CISO.~~
- Protect the administrative, supervisor, or root-level authentication information at the highest level demanded by the sensitivity of the system.
- Logon to his or her non-privileged account and then from that login to his or her privileged account to perform actions requiring privileges. For example, on a Unix operating system, the user must login to a non-privileged account before logging in as "root," and on a Microsoft Windows computer, the user must login to a non-privileged account before performing a privileged function that requires authentication as a privileged user.
- 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., e-mail, web browsing).

ML15056A494

- 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”~~
- 5 CFR Part 2635, “Standards of Ethical Conduct for Employees of the Executive Branch”
- 10 CFR Part 2, “Agency Rules of Practice and Procedure”
- 32 CFR Part 2002, “Controlled Unclassified Information”
- Committee on National Security Systems Issuances, <http://www.cnss.gov/>
- Executive Order 13103, “Computer Software Piracy”
- Executive Order 13526, “Classified National Security Information,” December 29, 2009.
- Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” October 07, 2011
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards, (FIPS), <http://csrc.nist.gov/publications/PubsFIPS.html>
- NIST Special Publications, <http://csrc.nist.gov/publications/PubsSPs.html>
- NRC Management Directive (MD) 2.7, “Personal Use of Information Technology”
- NRC MD 3.2, “Privacy Act”
- NRC MD 3.53, “NRC Records and Document Management Program”
- NRC MD Volume 12, “Security”
- NRC PII project home page <http://www.internal.nrc.gov/PII/index.html>
- 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>
- OMB Circular A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control”
- OMB Circular A-130, “Managing Information as a Strategic Resource”
- OMB memoranda
 - M-15-14, “Management and Oversight of Federal Information Technology”
 - M-16-04, “Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government”

- M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- ~~Public Law 99-474 (Title 18, United States Code), section 1030~~
- Public Law 113-187, "Presidential and Federal Records Act Amendments of 2014"
- Public Law 113-283, The Federal Information Security Modernization Act of 2014
- ~~Executive Order 13103, "Computer Software Piracy"~~
- ~~Executive Order 13526, "Classified National Security Information," December 29, 2009.~~
- ~~Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 07, 2011.~~
- ~~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-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"~~
 - ~~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"~~
- M-11-27, "Implementing the Telework Enhancement Public Law 113-291, Subtitle D—Federal Information Technology Acquisition Reform (FITARA)"
 - ~~Public Law 114-113, Cybersecurity Act of 2010: Security Guidelines"~~
 - ~~M-14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"~~

- ~~M 15 01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices~~
- Public Law 99-474 (Title 18, United States Code), section 1030
 - ~~M 15 13, Policy to Require Secure Connections across Federal Websites and Web Services~~
 - ~~M 15 14, Management and Oversight of Federal Information Technology~~
- ~~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 Tomeye"~~
 - ~~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"~~
 - ~~YA 12 0152, "Republication of NRC's Privacy Act Systems of Records Notices"~~
 - ~~YA 13 0014, "Reporting of Security Incidents, Infractions, and Violations"~~
- NRC Policy Memoranda

Formatted: List Bullet

ML15056A494

- "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 [CSOOCIO](#) Web pages
 - <http://www.internal.nrc.gov/CSO/policies.html>
 - <http://www.internal.nrc.gov/CSO/guidelines.html>
 - <http://www.internal.nrc.gov/CSO/procedures.html>
 - <http://www.internal.nrc.gov/CSO/processes.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>

APPENDIX B: GLOSSARY

<u>Authorizing Official (AO)</u>	<u>The individual(s) responsible for approving IT implementations for operation.</u>
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.

Formatted Table

<u>Designated Approving Authority (DAA)</u>	<u>The individual(s) responsible for approving IT implementations for operation.</u>
---	--

Electronic Media	Different types of data storage options. Electronic storage options change very quickly and include, but are not limited to, the following: <ul style="list-style-type: none"> • hard drives (i.e., both internal and external) • removable drives (e.g., external hard drives) • compact disks (CDs) • digital video disks (DVDs) • thumb drives • flash memory • floppy disks • magnetic tapes
------------------	--

Formatted Table

General User	A person with non-privileged 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	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
-------------	--

Non-Privileged Account	A user account with limited access privileges to an IT resource, such as those assigned to a general user. A non-privileged account cannot alter or bypass some or all of the security controls implemented for an IT resource.
------------------------	---

Non-public User	NRC employees, contractors, and other users that authenticate to NRC IT systems.
-----------------	--

ML15056A494

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 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 an IT resource, such as a system administrator or information system security officer. A privileged user may use and access privileged information on all or part of the resource. A privileged user may alter or bypass some or all of the security controls on an IT resource.
Sensitive Information	A generic term used to identify information designated as classified information, Safeguards information, or SUNSI. This includes any information or material, regardless of its physical form or characteristics, which is originated, owned, or possessed by the United States Government where a compromise of the confidentiality, integrity, or availability of the information could cause an adverse effect on government operations, government assets, or individuals.
User	Individual (general user, non-public user, or a privileged user) or process authorized to access an IT system.
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.