U.S. Nuclear Regulatory Commission
Agency-wide Rules of Behavior for Foreign Assignees
ML21175A037
Version 1.0, August 31, 2021

1. Introduction

The goal of the foreign assignee (FA) program is to exchange regulatory knowledge and nuclear safety and security expertise with the FA and the FA's regulatory body. These exchanges contribute to enhancing nuclear safety and security worldwide. Throughout the assignment, the expectation is that the FA will acquire an understanding of the U.S. nuclear regulatory process, technical bases, and regulatory requirements in the areas agreed to in the FA's work plan. Additionally, through interactions with NRC staff and completing work assignments, an FA learns the concepts of NRC's internal and external safety culture. NRC staff working with an FA learn from the exchange of expertise and the fresh viewpoints that an FA may provide. An FA may have a different regulatory philosophy and may offer helpful observations to NRC staff regarding U.S. regulations and procedures. In addition, an FA can provide NRC staff with a better understanding and knowledge of their respective nation's nuclear regulatory system. This knowledge enhances the NRC staff's perspectives and exposure to the international nuclear community.

2. Purpose

The purpose of the FA Agency-wide Rules of Behavior for Foreign Assignees is to appropriately protect the NRC's electronic information and computing resources. Each FA must acknowledge these rules of behavior.

3. Scope

The rules of behavior apply to all NRC FAs and the NRC staff who work with them.

4. Rules of Behavior for Foreign Assignees

The following rules apply to all NRC FAs. The signed Agency-wide Rules of Behavior for Foreign Assignees should be attached to the FA's approved security plan.

4.1 Information and Computing Resources

FAs shall:

1. Only use English writing when using NRC computing equipment. For example, all written documents, email, and other communications should only be written using the English language.
2. Incorporate an email signature that includes the FA's name and position for all transmissions via email.
3. Only access and use information related to the work agreed upon in the FA NRC invitation letter and defined in the FA NRC work plan and security plan. NRC recognizes that the work plan is meant to be a living document and may change throughout the assignment.

4. Use NRC-provided computing resources only for the work agreed upon in the FA NRC invitation letter and defined in the FA NRC work plan and security plan.
5. Assume responsibility for all actions performed and activities initiated using his or her user account.
6. Follow the FA's NRC supervisor established procedures for accessing information, including the use of user identification (User-ID), authentication information (e.g., personal identification numbers, passwords, digital certificates), and other physical and logical safeguards.
7. Follow the FA's NRC supervisor established procedures for requesting and disseminating information.
8. Access only those files, directories, and applications for which the user has been granted access authorization in accordance with the FA's security plan.
9. 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 privacy screens, hoods, or positioning the equipment (e.g., monitors) so that they face away from doorways, windows, or open areas.
10. Log off (sign out) all equipment and sessions when leaving equipment for the day and terminate sessions or employ a session-locking mechanism that requires user re-authentication to regain session access before leaving equipment unattended.

FAs shall NOT:

1. Remove NRC computing equipment from NRC facilities without written authorization from the FA's NRC supervisor that specifies the specific dates and purposes for which removal of the equipment from NRC facilities is authorized (e.g., travel to a Regional Office or a nuclear facility site; and work from home, which could be approved on a case by case basis).
2. Provide non-NRC individuals with access to NRC computing equipment.
3. Share NRC information with those not authorized by NRC to access the information.
4. Use NRC computing resources for commercial purposes; in support of "for-profit" or "non-profit" activities; or in support of a business, outside employment, or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).
5. Use NRC computing resources for fund-raising activities, endorsing any product or service, participating in any lobbying activity, or engaging in any political activity (e.g., including sending e-mail messages endorsing partisan political groups or candidates for partisan political office).
6. Use NRC computing resources for any use that causes congestion, delay, or disruption of service to any agency system or equipment. Examples of possible misuse include sending large file attachments that can degrade the performance of the network, such as video or audio files.
7. Use NRC computing resources for activities that stop, interrupt, or interfere with NRC's mission or operations.
8. Use NRC computing resources in a way that my result in loss of employee productivity.

9. Allow anyone else to use their computer while they are logged into the system except where an NRC authorized 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.
10. Place software onto an NRC computing resource.
11. Connect a computing resource (e.g., cellular phone, Universal Serial Bus (USB) drive) to any NRC system, including infrastructure systems, such as the LAN.
12. 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.
13. 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.
14. Bypass system controls or access data for any reason other than official duties.

4.2 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 FAs shall:

1. Protect authentication information (e.g., passwords, private keys, personal identification numbers) at a level commensurate with the sensitivity level or classification level and classification category of the information to which the authentication allows access.
2. Promptly change authentication information whenever compromise is known or suspected.
3. Select and use unique authentication information for access to each computing resource or group of computing resources subject to applicable authentication information restrictions.
4. Notify their NRC FA supervisor when experiencing difficulties with a user account or authentication information.
5. Report any suspected or known authentication information (e.g., password, digital certificate) compromise to the system Information System Security Officer (ISSO) and to their NRC FA supervisor.

FAs shall NOT:

1. 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.

2. Attempt to bypass or circumvent access controls to a computing resource.
3. Store authentication information in writing or on-line (including password saving features of operating systems and applications), except:
    a. In the case of initial use and reset authentication information or
    b. Where an NRC authorizing official-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.
4. Use the same authentication information (e.g., passwords, private keys, personal identification numbers) for NRC system access and non-NRC purposes.

4.3 Electronic Data Protection

The FA 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 the FA security plan.

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

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

1. Understand that Internet and e-mail use may be monitored, and by signing these rules of behavior consent to such monitoring.
2. Acknowledge that any information on a United States Government system is the property of the United States Government and may become an official record.
3. Only use their NRC government e-mail address for NRC authorized purposes.

FAs use of the NRC Internet, Messaging, Telephones, Collaboration Tools, Conferencing, Video, and e-mail services and resources shall NOT:

1. Automatically forward NRC e-mail or other messaging to any account that is not an NRC email account.
2. Send NRC sensitive information to unauthorized accounts.
3. Use these capabilities for fraudulent or harassing messages or for sexual remarks or the downloading of illegal or inappropriate materials (e.g., pornography).
4. 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 government services.
5. Share information with a third country outside the FA country of origin.

4.5 Protection of Computing Resources

NRC reserves the right to access or confiscate NRC equipment at any time. FAs use of NRC computing resources to process NRC information or to connect to NRC systems shall:

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

FAs shall NOT:

1. Make any changes to an NRC computing resource's system configuration, except for user display preferences, unless directed to do so by an authorized NRC system administrator.
2. Program a computing resource with NRC sign-on sequences, NRC passwords or other authentication information, or NRC access phone numbers.
3. Use wireless solutions and configurations that are not specifically approved by their NRC FA supervisor.

4.6 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.

FAs will report actual and suspected incidents immediately (within one hour) to their NRC FA supervisor. Examples of incidents include:

1. Messages that warrant attention beyond deletion.
2. Receipt of obscene, racist, profane, libelous, or offensive messages.
3. Unusual phone calls (e.g., soliciting personal or IT system information).
4. Automatic installation of unknown software.
5. Requests for user identification and authentication information.
6. Computer use in NRC facilities by unknown or unidentified individuals.
7. Losses or compromises of Personally Identifiable Information (PII).
8. Requests for information from a third-party or country.

5. Rules of Behavior for NRC Staff Who Work with Foreign Assignees

The following rules apply to all NRC staff who work with FAs.

5.1 Information and Computing Resources

NRC staff who work with FAs shall:

1. Only provide FAs with access to information related to the work agreed upon in the FA NRC invitation letter and defined in the FA NRC work plan and security plan.
2. Only communicate with FAs using English when using NRC computing equipment. For example, all written documents, email, and other communications should only be written using the English language.
3. Follow established procedures for providing FAs with access to information, including the use of User-ID, authentication information (e.g., personal identification numbers, passwords, digital certificates), and other physical and logical safeguards.
4. Follow established FA procedures for requesting and disseminating information.
5. Provide the FA with access to 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.

APPENDIX A: GLOSSARY

Computing Resource	Computers and IT resources, including desktop and laptop computers, networks, facilities, printers, scanners, faxes, Personal Electronic Devices (PEDs), cell phones, electronic media, printouts, and any other IT used to store or process information.
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., external hard drives) • compact disks (CDs) • digital video disks (DVDs) • thumb drives • flash memory • floppy disks • magnetic tapes
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.
Sensitive Information	A generic term used to identify 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.

U.S. Nuclear Regulatory Commission
Agency-wide Rules of Behavior for Foreign Assignees

Acknowledgement Statement

By my electronic acknowledgement, I understand and consent to the following when accessing the information systems operated by or on behalf of U.S. Nuclear Regulatory Commission (NRC), which include: (1) NRC computers; (2) the NRC network; (3) all computers connected to the NRC network; and (4) all devices (e.g., smartphones, tablets) and storage media (e.g., thumb drive, flash drive) attached to the NRC network or to a computer on the NRC network or having access to NRC electronic information:

- I am accessing a U.S. Government information system that is provided for U.S. Government-authorized use only. No other unofficial use is authorized.
- The Government routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At anytime, the government may for any lawful government purpose monitor, intercept, search or seize any communication or data transiting or stored on this information system;
- Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

I acknowledge that I have read the Agency-wide Rules of Behavior for Foreign Assignees, and will comply with the terms, procedures, and rules governing the use and access to the NRC information technology resources.

Name	**Signature and Date**