STATEMENT OF EMPLOYEE INFORMATION SECURITY RESPONSIBILITIES

Forest Service (FS) employees are granted access to information resources in order to facilitate their FS job responsibilities. FS employees must understand and agree to their Information Security Responsibilities to be allowed access to information systems.

I acknowledge that I understand and agree to comply with user responsibilities as stated in Forest Service Manual (FSM) Chapter 6680, *Security of Information, Information Systems, and Information Technology*. If I do not understand a requirement, I will ask my supervisor for clarification. I understand that I also must comply with United States Department of Agriculture policies and procedures, and with federal, state, and local laws.

I understand that I must complete a Computer Security Awareness course every year, and that, depending on my job, I may be required to take additional role based information security training. In addition, I understand that I am required to successfully complete periodic refresher training at least annually and as requested.

Key elements of FSM Chapter 6680, for which I am responsible, are summarized below. I understand and agree that I must periodically review the chapter for changes.

I am responsible to:

- Acknowledge individual accountability on all FS information systems by clicking OK on the System Use Notification Banner during each logon process. The logon banner reaffirms every user's acceptance of the terms of use for all FS information systems.
- Only accessing data for which I have authorized access.
- Take appropriate measures to protect information from unauthorized access, including seeking out and applying security measures to protect sensitive information stored on my computer, on other electronic devices, or on other media such as CDs, DVDs, magnetic tape, and paper (FSM 6683.04f).
- Take extra measures to ensure the protection of media in transit or stored on removable media. I must appropriately secure removable media, equipment, and information system output with a lock or otherwise secured container. Media-especially, but not limited to, media containing PII-will be transported outside of a FS facility both physically secured and logically secured (encrypted). Any data leaving FS facilities, including via the internet and E-mail, must be secured with FS approved encryption standard.
- Not removing Agency information or data from FA facilities without explicit approval from a supervisor and adherence to encryption requirements.
- Not store any classified information on my computer.
- Encrypt, using agency authorized encryption methods, any government sensitive or confidential information or information subject to the Privacy Act that is stored on any personal electronic device or removable storage medium.
- Sign off or electronically lock the computer before leaving it unattended (FSM 6683.04f)
- Comply with physical security standards and procedures specified in section 6683.15a of FSM Chapter 6680, including taking appropriate measures to protect computer equipment and other electronic devices from theft, damage, or unauthorized use.

- Keep personal use of telecommunications and information resources and equipment within the limits set by section FSM 6683.15b, *Limited Personal Use*, and to understand what constitutes inappropriate use as specified in section FSM 6683.15d, Inappropriate Personal Uses.
- Comply with password standards and procedures specified in section FSM 6684.12, and FSM 6684.12, Exhibit 1.
- Not sharing, writing down, or otherwise transferring my password to an unauthorized user. My password is for my use only. Sharing passwords violates accountability, which requires that every action in an information system be traceable to a single user.
- Verify that the automatic virus definition file updates to the enterprise antivirus tool installed on my computer(s) (currently, Symantec AntiVirus) occur as scheduled (FSM 6683.04f).
- Store corporate data within the corporate filing system, where it is backed up routinely (FSM 6683.04f). The FS defines corporate data as information owned, collected, maintained, or generated by the enterprise that has inherent value to and is intended for consistent, shared use within the enterprise. (FSM 6680.5).
- Install only that software, including "freeware" and "shareware," for which I have obtained authorization. When my privileges are elevated to allow installation of authorized software, I will perform only those activities that are specifically authorized (FSM 6683.04f).
- Being aware of the proper procedures for the sanitization and disposal of Agency information and data. I am aware that data can be retrieved from media (diskettes, tapes, hard drives, or other memory devices) even after being 'erased' or 'deleted'. To properly sanitize media of residual data I must contact the Helpdesk for assistance in degaussing, overwriting, or otherwise ensuring media is purged prior to disposal.
- Being aware of retention and disposal requirements of data to which I have access privileges.
- Ensure that Agency sensitive information to which I have access is securely maintained, disseminated, and protected from disclosure, release, or extraction to unauthorized individuals or groups. In the instance of information protected by specific laws, such as the Privacy Act or the Health Insurance Privacy and Portability Act (HIPPA), users must be aware of the confidentiality protection procedures required of them in their handling of agency sensitive data as required by law.
- Not removing hardware containing Agency sensitive information from FS without following appropriate media protection (encryption) or sanitization and disposal (overwriting, degaussing) procedures.
- Take FS computer equipment from a FS facility only for official business purposes.
- Only use computer equipment for which I have authorization.
- Not moving or installing computer equipment unless I am an authorized technician and the action has been approved by the appropriate IT System Owner or supervisor.
- Ensure if I am working remotely to follow the remote access requirements, which may include two-factor authentication and additional restrictions on portable computer systems to ensure these devices do not compromise the integrity or confidentiality of FS information or data.

- Not change the configuration settings or attempt to modify or disable any of the security programs installed on their FS information system, including virus protection software and the password protected screen saver.
- Ensure all software in use by a user on FS equipment must have a valid license on file with purchasing.
- Promptly report all suspected security incidents to the FS Computer Incident Response Team (CIRT@FSNOTES) and/or my supervisor or other appropriate management official(s) (FSM 6683.04f).
- Understand the consequences for non-compliance behavior regarding the ROB.
- Ensure dial in remote access is turned off or disconnected when not in use.
- Comply with defined and proper Internet usage guidelines.
- Comply with proper usage of search functions with in databases.

Personally Identifiable Information (PII) is any piece of information which can potentially be used to uniquely identify, contact, locate, or impersonate a single person. If I have access to PII I am responsible to:

- Never access PII unless absolutely necessary to perform my job.
- Never disclose PII to another person within FS unless they have verified that the other person is entitled to the information.
- Never remove PII from FS premises unless it is encrypted using a FS approved method unless they have a copy of a memorandum waiving the encryption requirement that has been signed by a Business Unit Manager and that applies to this circumstance.
- Verify that any time I extract any PII from an IT system into a computer readable form, e.g., into a spreadsheet or report, that this act has been properly logged so that the location of the PII may be tracked.
- Ensure that after having finished using any extracted PII, or after 90 days, whichever comes first, I will erase the PII or receive written permission from my supervisor to retain it for longer.
- Ensure when erasing PII, that this act is properly logged so that the location of the PII will no longer be tracked.
- Never access PII from computers or devices outside of FS premises without advance authorization for remote access.
- Never attempt remote access without using approved FS access methods, which generally require the use of a SecurID device (called a “token”).
- Never store their token with or near a laptop or other portable computer that contains PII or is used for PII access.
- Never mark their token with any information such as name or password.
- Promptly report any possible, suspected, or actual loss of PII or any device containing PII to the appropriate point of contact. Hence, I must ensure that I know how to make a report, and that I keep a record of the reporting point of contact separately from any device, so that a report is made if the device is missing.
- Report any possible, suspected, or actual loss of PII or any device containing PII within 15 minutes of discovery of the incident, regardless of the time of day.
- Physically secure all portable devices containing PII. I will lock up laptops using a cable lock when they are not in use, including when they are within their home, vehicle, or

hotel room. I will lock small devices into secure containers when they are not in their possession.
- Encrypt PII when it is placed onto removable media such as CDs, "thumb drives" or memory sticks and when it is removed from agency premises.
- Ensure that if PII is lost or stolen, it is reported to the Helpdesk within 24 hours.

I understand that any use of Forest Service communications resources generally is not secure, is not private, and is not anonymous, and that system managers do employ monitoring tools to detect improper use (FSM 6683.15i, 6684.3). I understand that there is no right to privacy when using government information systems (logon warning banner).

I understand that non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. I understand that findings of culpability will result in disciplinary action consistent with the provision of FSM 6170 and DPM 751, which may include the loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use.

STATEMENT OF INFORMATION SECURITY RESPONSIBILITIES FOR ASSOCIATE USERS OF FOREST SERVICE SYSTEMS

Forest Service (FS) cooperators, volunteers, contractors, and other associates are granted access to information resources in order to facilitate their Forest Service related responsibilities. FS associates must understand and agree to their Information Security Responsibilities to be allowed access to information systems.

I acknowledge that I understand and agree to comply with user responsibilities as stated in FSM Chapter 6680, *Security of Information, Information Systems, and Information Technology* (http://www.fs.fed.us/cgi-bin/Directives/get_dirs/fsm?6600!.). If I do not understand a requirement, I will ask for clarification.

I understand that I also must comply with United States Department of Agriculture (USDA) policies and procedures, and with federal, state, and local laws. I understand that as a FS associate, I may not be entitled to the same limited personal use privileges as FS employees, and that my use of FS information systems and equipment is limited to that which is specifically described in my contract or other agreement with the Forest Service.

I understand that my contract or other agreement may specify additional information security responsibilities or requirements, such as the need for a signed confidentiality statement.

I understand that I am required to complete Forest Service Information Security Awareness courses, and may be required to take additional role-based security training, depending on my job. In addition, I understand that I am required to successfully complete periodic refresher training at least annually and as requested.

Key elements of Forest Service Manual (FSM) Chapter 6680, for which I am responsible, are summarized below. I understand and agree that I must periodically review the chapter for changes.

I am responsible to:

- Take appropriate measures to protect information from unauthorized access, including seeking out and applying security measures to protect sensitive information stored on my computer, on other electronic devices, or on other media such as CDs, DVDs, magnetic tape, and paper (FSM 6683.04f).
- Not store any classified information on my computer.
- Encrypt, using agency authorized encryption methods, any government sensitive or confidential information or information subject to the Privacy Act that is stored on any personal electronic device or removable storage medium.
- Sign off or electronically lock the computer before leaving it unattended (FSM 6683.04f)
- Comply with physical security standards and procedures specified in section 6683.15a of FSM Chapter 6680, including taking appropriate measures to protect computer equipment and other electronic devices from theft, damage, or unauthorized use.
- Comply with password standards and procedures specified in section FSM 6684.12, and FSM 6684.12, Exhibit 1 of Interim Directive 6680-2005-3.

- Verify that the automatic virus definition file updates to the enterprise antivirus tool (currently, Symantec AntiVirus) occur as scheduled (FSM 6683.04f).
- Store corporate data within the corporate filing system, where it is backed up routinely (FSM 6683.04f). The FS defines corporate data as information owned, collected, maintained, or generated by the enterprise that has inherent value to and is intended for consistent, shared use within the enterprise.(FSM 6680.5).
- Install only that software for which I have obtained authorization, and when my privileges are elevated to allow installation of authorized software to perform only those activities that are specifically authorized (FSM 6683.04f).
- Refrain from installing on FS computer equipment any software; including "freeware" and "shareware," that does not have approval from the Chief Information Office (FSM 6683.15h).
- Be aware of the proper procedures for the sanitization and disposal of Agency information and data. Users shall be aware that data can be retrieved from media (diskettes, tapes, hard drives, or other memory devices) even after being 'erased' or 'deleted'. To properly sanitize media of residual data users must contact the Helpdesk for assistance in degaussing, overwriting, or otherwise ensuring media is purged prior to disposal.
- Being aware of retention and disposal requirements of data to which I have access privileges.
- Ensure that Agency sensitive information to which I have access is securely maintained, disseminated, and protected from disclosure, release, or extraction to unauthorized individuals or groups. In the instance of information protected by specific laws, such as the Privacy Act or the Health Insurance Privacy and Portability Act (HIPPA), users must be aware of the confidentiality protection procedures required of them in their handling of agency sensitive data as required by law.
- Not remove hardware containing Agency sensitive information from FS without following appropriate media protection (encryption) or sanitization and disposal (overwriting, degaussing) procedures.
- Take FS computer equipment from a FS facility only for official business purposes.
- Only use computer equipment for which I have authorization.
- Not move or install computer equipment unless I am an authorized technician and the action has been approved by the appropriate IT System Owner or supervisor.
- Ensure if I am working remotely (those who operate portable computer systems in an alternate workplace i.e. cell phone, PDA (Blackberry), home computers), I take the same precautions as required of users of stationary systems located at FS facilities to protect the FS systems' hardware, software, and information.
- Ensure if I am working remotely to follow the remote access requirements, which may include two-factor authentication and additional restrictions on portable computer systems to ensure these devices do not compromise the integrity or confidentiality of FS information or data.
- Not change the configuration settings or attempt to modify or disable any of the security programs installed on their FS information system, including virus protection software and the password protected screen saver.
- Ensure all software in use by a user on FS equipment must have a valid license on file with purchasing.

- Understand findings of culpability will result in disciplinary action consistent with the provisions of FSM 6170 and DPM 751, which may include the loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use.
- Promptly report all suspected security incidents to the FS Computer Incident Response Team (CIRT@FSNOTES) and/or my supervisor or other appropriate management official(s) (FSM 6683.04f).

Personally Identifiable Information (PII) is any piece of information which can potentially be used to uniquely identify, contact, locate, or impersonate a single person. If I have access to PII I am responsible to:

- Never access PII unless absolutely necessary to perform my job.
- Never disclose PII to another person within FS unless they have verified that the other person is entitled to the information.
- Never remove PII from FS premises unless it is encrypted using a FS approved method unless they have a copy of a memorandum waiving the encryption requirement that has been signed by a Business Unit Manager and that applies to this circumstance.
- Verify that any time I extract any PII from an IT system into a computer readable form, e.g., into a spreadsheet or report, that this act has been properly logged so that the location of the PII may be tracked.
- Ensure that after having finished using any extracted PII, or after 90 days, whichever comes first, I will erase the PII or receive written permission from my supervisor to retain it for longer.
- Ensure when erasing PII, that this act is properly logged so that the location of the PII will no longer be tracked.
- Never access PII from computers or devices outside of FS premises without advance authorization for remote access.
- Never attempt remote access without using approved FS access methods, which generally require the use of a SecurID device (called a “token”).
- Never store their token with or near a laptop or other portable computer that contains PII or is used for PII access.
- Never mark their token with any information such as name or password.
- Promptly report any possible, suspected, or actual loss of PII or any device containing PII to the appropriate point of contact. Hence, I must ensure that I know how to make a report, and that I keep a record of the reporting point of contact separately from any device, so that a report is made if the device is missing.
- Report any possible, suspected, or actual loss of PII or any device containing PII within 15 minutes of discovery of the incident, regardless of the time of day.
- Physically secure all portable devices containing PII. I will lock up laptops using a cable lock when they are not in use, including when they are within their home, vehicle, or hotel room. I will lock small devices into secure containers when they are not in their possession.
- Encrypt PII when it is placed onto removable media such as CDs, “thumb drives” or memory sticks and when it is removed from agency premises.
- Ensure that if PII is lost or stolen, it is reported to the Helpdesk within 24 hours.

WFDSS RULES OF BEHAVIOR

I understand that any use of Forest Service communications resources generally is not secure, is not private, and is not anonymous, and that system managers employ monitoring tools to detect improper use (FSM 6683.15i). I understand that there is no right to privacy when using government information systems (logon warning banner).

I understand that if I have been granted authorization to use my own or my organization's computer equipment, I must complete and sign (or a representative of my organization must complete and sign on my behalf) the **FS Standards for Associate-Owned PCs Used for Forest Service Work and Connected to the FS Network.**

I understand that non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions taken will be determined by each user's specific agency with recommendation of the Contracting Officer/Contracting Officer's Technical Representative, in collaboration with Information System Security Officer and/or USDA National Information Technology Center Security Officer (NITC). Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or request of removal/termination, depending on the severity of the violation.

STATEMENT OF INFORMATION SECURITY RESPONSIBILITIES FOR USERS WITH PRIVILEGED ACCESS TO INFORMATION SYSTEMS

Employees or contractors entrusted with responsibilities for administering information systems, or other privileged access to information systems, have a particularly important role in protecting the systems they access or administer and the Forest Service (FS) General Support System (GSS). FS employees and contractors with privileged access must understand and agree to their Information Security Responsibilities to be allowed privileged access or to administer FS information systems.

I understand that I am required to complete Forest Service Information Security Awareness courses, and may be required to take additional role-based security training, depending on my job. In addition, I understand that I am required to successfully complete periodic refresher training at least annually and as requested.

I acknowledge that I understand and agree to comply with user responsibilities as stated in Forest Service Manual (FSM) Chapter 6680, *Security of Information, Information Systems, and Information Technology*, and Interim Directives that supplement this chapter. If I do not understand a requirement, I will ask my supervisor for clarification. I understand that I also must comply with United States Department of Agriculture (USDA) policies and procedures, and with federal, state, and local laws.

Key elements of Forest Service Manual (FSM) Chapter 6680, for which I am responsible, are summarized below. I understand and agree that I must periodically review the chapter for changes.

- I understand that, in addition to this document, I must understand and sign the Statement of Employee Security Responsibilities or the Statement of Information Security Responsibilities for Associate Users of Forest Service Systems.
- I understand that I have been granted enhanced privileges in order to perform specific functions on information systems that are part of a FS GSS, and that these privileges are to be used only to perform my assigned job responsibilities.
- I will not use my privileges to grant myself or any other person unauthorized privileges, or to modify any access accounts, privileges, system configurations, or data in an unauthorized manner.
- I understand that I have a special duty to safeguard FS information resources, and will implement and operate enterprise measures to protect those resources, as instructed by technical information bulletins (TIB), standard operating procedures, or other directives.
- I will exercise maximum care in protecting the enhanced access credentials with which I have been entrusted.
- I understand that privileged access to FS information systems may be changed or revoked at the discretion of management, and may be modified as roles and responsibilities change.

- I will promptly report all suspected security incidents to the FS Computer Incident Response Team (CIRT@FSNOTES) and/or my supervisor or other appropriate management official(s) (FSM 6683.04f).
- I will protect "privileged accounts passwords" at the highest level demanded by the sensitivity level of the system (Privileged accounts passwords include the supervisor, root, and administrator or equivalent, passwords).
- I will not divulge, to any person outside of the FS, the numbers of Dial-up or Dial-back modem phone.
- I will not use my privileged access to develop or run programs that are NOT for work purposes.
- I will not download, install, or run programs or utilities that reveal weaknesses in the security of the system, such as password cracking programs, on FS computing systems. Such programs or tools may only be used by approved personnel, and may ONLY be run with explicit authorization and written rules of engagement that include a specific time and chain of authority for stopping the procedure.
- I will help train users on the appropriate use and security of the information system.
- I will monitor information system activity, including the execution of unscheduled or unauthorized programs.
- I will ensure that malicious code protection for servers, both internal and externally accessible, is in place and current.
- I understand findings of culpability will result in disciplinary action consistent with the provisions of FSM 6170 and DPM 751, which may include the employee's loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use.

Personally Identifiable Information (PII) is any piece of information which can potentially be used to uniquely identify, contact, locate, or impersonate a single person. If I have access to PII I am responsible to:

- Never access PII unless absolutely necessary to perform my job.
- Never disclose PII to another person within FS unless they have verified that the other person is entitled to the information.
- Never remove PII from FS premises unless it is encrypted using a FS approved method unless they have a copy of a memorandum waiving the encryption requirement that has been signed by a Business Unit Manager and that applies to this circumstance.
- Verify that any time I extract any PII from an IT system into a computer readable form, e.g., into a spreadsheet or report, that this act has been properly logged so that the location of the PII may be tracked.
- Ensure that after having finished using any extracted PII, or after 90 days, whichever comes first, I will erase the PII or receive written permission from my supervisor to retain it for longer.
- Ensure when erasing PII, that this act is properly logged so that the location of the PII will no longer be tracked.
- Never access PII from computers or devices outside of FS premises without advance authorization for remote access.

- Never attempt remote access without using approved FS access methods, which generally require the use of a SecurID device (called a "token").
- Never store their token with or near a laptop or other portable computer that contains PII or is used for PII access.
- Never mark their token with any information such as name or password.
- Promptly report any possible, suspected, or actual loss of PII or any device containing PII to the appropriate point of contact. Hence, I must ensure that I know how to make a report, and that I keep a record of the reporting point of contact separately from any device, so that a report is made if the device is missing.
- Report any possible, suspected, or actual loss of PII or any device containing PII within 15 minutes of discovery of the incident, regardless of the time of day.
- Physically secure all portable devices containing PII. I will lock up laptops using a cable lock when they are not in use, including when they are within their home, vehicle, or hotel room. I will lock small devices into secure containers when they are not in their possession.
- Encrypt PII when it is placed onto removable media such as CDs, "thumb drives" or memory sticks and when it is removed from agency premises.
- Ensure that if PII is lost or stolen, it is reported to the Helpdesk within 24 hours.

I understand that non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. I understand that findings of culpability will result in disciplinary action consistent with the provision of FSM 6170 and DPM 751, which may include the loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use. In addition, for contractors, actions taken will be determined by each user's specific agency with recommendation of the Contracting Officer/Contracting Officer's Technical Representative, in collaboration with Information System Security Officer and/or USDA National Information Technology Center Security Officer (NITC). Actions may include (but may not be limited to) a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or request of removal/termination, depending on the severity of the violation.