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.

Employee or Contractor Name (typed or printed)

Employee or Contractor Signature Date

Supervisor or CO/COR Name (typed or printed)

Supervisor or CO/COR Signature Date