



Rules of Behavior Forest Stewardship Program WebDET/WinDET

Introduction:

Computer security is part of your job. The following rules of behavior are to be followed by all users of WebDET/WinDET. The rules clearly delineate responsibilities of and expectations for all individuals with access to WebDET/ WinDET. Non-compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination. Once notified of rules, individuals are accountable for their actions.

Responsibilities:

Security Officers.--The WebDET/ WinDET Security Officer is responsible for ensuring an adequate level of protection is afforded to WebDET/ WinDET, through an appropriate mix of technical, administrative, and managerial controls. The Security Officer develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot-checks to determine that an adequate level of compliance with security requirements exists. The Security Officers (primary and alternate) are responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in the WebDET/ WinDET security posture.

Unit Managers.--Unit managers or their designees will ensure that personnel are assigned access roles in WebDET/ WinDET commensurate with their business responsibilities and their training in use of the system.

Users of WebDET.--Users of WebDET/ WinDET will support the security and data integrity of WebDET by following all rules and procedures agreed to by signing the User Agreement form (Non-disclosure Agreement), and as indicated below.

Other Policies and Procedures:

System-specific rules of behavior are established as needed by each system owner. Instances of non-compliance with established rules of behavior are handled on a case-by-case basis by appropriate management officials. Guidance provided to WebDET/WinDET users states:

Only authorized users are permitted access to USDA computer resources. Accessing or attempting to access computer resources without authority is illegal. Disclosing sensitive information, such as Privacy Act data, is not authorized except as provided for official business.

Unless authorized, system maintenance [including NITC, FS-AHE, FS-ISO, and WebDET/ WinDET team] personnel are not permitted to alter or disable system, application, or database security controls.

WebDET/WinDET users security responsibilities – The Security Staff are the authority in security matters, but day-to-day security is a shared responsibility for all WebDET/ WinDET users. Some things every WebDET/ WinDET -authorized user is responsible for include:

Sharing logon IDs or passwords – The use of personal logons and passwords ensures individual accountability. Unless special provisions have been made, and approvals received, logons or passwords are not shared.

Protecting data – Back up files regularly. One way to make this easy to do is to keep data in a specific subdirectory (e.g., c:\data), and to back up non-sensitive data by copying it to the LAN or an external hard drive.

Providing application and data security for WebDET/ WinDET customers – The WebDET/ WinDET Security Officer (primary and alternate) will ensure that users and WebDET/ WinDET data are appropriately protected. Available security controls are used and others added, if necessary. Security controls are never bypassed, unless required in writing, by our customers for business reasons.

Watch for security incidents and report them to the WebDET/ WinDET Security Staff – WebDET/ WinDET users must watch for anomalies that may indicate an intrusion has taken place, or is being attempted. They are familiar with possible indications that an incident has taken place. Incident reporting policy is followed.

Protect sensitive computer output – Sensitive documents must be shredded and not placed in recycle bins. CDs and Diskettes not formally degaussed must be destroyed.

Guard against computer viruses – Desktop computers are set to boot first from the C drive, and then from the A drive. This will avoid catching boot sector viruses by accidentally trying to boot from an infected diskette. Periodically scan hard drives, and new data or program diskettes. I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for WebDET/ WinDET.

Print Name	Signature	FS Unit or State	Date

Mail completed form with **original signature** to:

Cindy Barnett
U.S. Forest Service
180 Canfield Street
Morgantown, WV 26505

10.15.2009