

SUBJECT: USDA Internet Access

APPROVED: 10/01/98

1 PURPOSE

Use of the Internet by the National Appeals Division (NAD) employees and contractors while using government-owned equipment, facilities, Internet addresses, or domain names registered to NAD.

2 AUTHORITY

Departmental Regulation 3140-2, USDA Internet Security Policy.

3 BACKGROUND

The Internet is comprised of thousands of interconnected networks which provide digital pathways to millions of information sites. Because these networks subscribe to a common set of standards and protocols, users have worldwide access to Internet hosts and their associated applications and databases. Electronic search and retrieval tools permit users to gather information and data from a multitude of sources and to communicate with other Internet users who have related interests.

Access to the Internet provides government agencies with the opportunity to locate and use current and historical data from multiple sources worldwide in their decision-making processes.

4 POLICY

a Scope

- (1) This policy applies to Internet access only. It does not cover the requirements, standards, or procedures for the development and implementation of NAD information sites on the Internet.
- (2) NAD Internet users covered by this policy are full or part-time employees, and Division contractors who are authorized to use government-owned equipment or facilities.

b Use

Federal computer systems are used to conduct official government business only.

The following restrictions apply to use of the Internet on government-owned equipment or facilities:

- (1) Accessing, retrieving, or printing text and graphics information which exceeds the bounds of generally accepted standards of good taste and ethics.
- (2) Engaging in unlawful activities or any other activity which would in any way bring discredit to the Division.
- (3) Engaging in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.
- (4) Engaging in any activity which would compromise the security of any government host computer. Host log-in passwords will not be disclosed or shared with other users.
- (5) Engaging in any fund raising activity, endorsing any products or services, participating in any lobbying activity, or any active political activity.

c Supervisory Responsibilities

Supervisors are responsible for providing adequate guidance and education to employees on the appropriate use of the Internet.

d User Responsibilities

Users are responsible for:

- (1) Learning about and following security procedures in their use of Internet services and refraining from any practices which might jeopardize the Division's computer systems and data files including, but not limited to, virus attacks when downloading files from the Internet.
- (2) Learning about Internet etiquette, customs, and courtesies including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
- (3) Familiarization with any special requirements for accessing, protecting, and utilizing data, including Privacy Act materials, copyrighted materials, and procurement sensitive data.

- (4) Performing in a way that reflects positively on the Division, since they are identified as NAD employees on the Internet.

Individuals using government equipment with access to the Internet are subject to having activities monitored by system or security personnel. Use of this system constitutes consent to security monitoring, and employees should remember that sessions on the Internet may not be private.