Telecommuting Policy

Telecommuting is a method of reducing air pollution, reducing congestion, conserving energy, increasing employee productivity and efficiency, and retaining a creative, experienced, and diverse work force. This policy is intended to apply to formalized, contractually-agreed upon telecommuting projects where working at an alternate location is a routinely scheduled occurrence. It is not intended for ad hoc, short-term situations where employees work at home on special occasions to complete specific projects.

Recommended Policy

1. Telecommuting is neither a universal employee right nor a universal employee benefit; telecommuting is a management option which may be made available to some employees when a mutually beneficial situation exists for USDA, the agency, and the employee. Telecommuting contracts may be terminated at any time the beneficial situation ceases to exist for USDA, Departmental Administration or the staff office.
2. Employees do not have an obligation to telecommute nor can they be compelled to telecommute. An employee may return to the conventional office arrangement at any time if they wish to withdraw from telecommuting.
3. Each agency must establish a telecommuting policy within the framework of the Departmental Administration policy.
4. Every DA employee involved in a formal telecommuting project must complete and agree to a telecommuting agreement.
5. Telecommuting employees should be encouraged to use DA-supplied computers for telecommuting, if feasible. No DA employee should be compelled to use privately-owned computer equipment. If DA equipment is used, the employee must exercise reasonable care for the equipment. The employee may be held liable for damage caused by negligence. If employee-supplied computers are used, the employee must release USDA and DA from any and all liability.
6. Telecommuting employees must comply with all applicable laws, state administrative rules, USDA, and agency rules. The employee may not copy or distribute USDA/DA/NFC/-provided software. The employee may not install unauthorized hardware or software on Departmental Administration owned equipment.

Telecommuter Rules and Policies

Each agency and its employees shall comply with computer software licensing agreements and federal laws, including copyright and patent laws. DA-IRD or the respective staff office will provide enough legally purchased copies of computer software to enable all employees to meet managements expectations and reduce potential for computer software piracy.

Information Technology Security

1. Establish a level of security that is consistent with the value and sensitivity of the information technology asset as it exists in DA.
2. anyone who accesses a computer network that:

   a. Unauthorized use may result in prosecution; and

   b. Electronic mail is non-confidential;

   c. Require each employee, contractor and anyone else who is given access to an information technology asset to certify that he understands:

   I. The proper use of the information technology asset; and

II. His obligation to protect the information technology asset.

Recommendations for Telecommuting Security

POINT OF ENTRY VALIDATION (Dial-In Only)

1. Only dial-in to systems specifically set-up for telecommuting.
2. Knowledge of dial-in numbers should be limited.
3. Encryption should be used as the situation requires.
4. Daily access logs will be created indicating time and duration on connection.
5. File servers that telecommuters attach to should be physically and logically isolated.
6. An additional password may be required at point of entry for dial in users.
7. Call-back systems may be employed for telecommuters requiring access to files residing on the network.

NETWORK SECURITY

1. Each PC must be kept secure.
2. Login ID's should be assigned only to authorized employees and those authorized to access to Departmental Administration resources.
3. Each Login ID must have a password.
4. Passwords should be changed every 90 days.

SECURITY POLICIES

1. Confidential data may be used at home. Each staff office must have appropriate policies regarding confidential data use at home. OCR and OHRM may want to restrict further
2. Access to confidential information must be limited and the employee must comply with USDA/DA/staff office rules regarding confidential information.
3. All diskettes and files downloaded from the Internet must be scanned for viruses.
4. Agency data may be uploaded and downloaded.

PHYSICAL SECURITY

1. Password protected screen savers and password protected booting should be used. Diskettes and papers should be kept in a locked, secure place.
2. Surge protectors should be used by all telecommuters.