

Directive

3300.1

3/19/07

USE OF GOVERNMENT OFFICE EQUIPMENT

I. PURPOSE

This Directive establishes Agricultural Marketing Service (AMS) policy on the use of Government office equipment.

II. REPLACEMENT HIGHLIGHTS

This Directive replaces AMS Directive 3300.1, Use of Government Office Equipment, dated 2/9/01. Changes are marked with asterisks.

III. BACKGROUND

A. Government office equipment (which includes e-mail and the Internet) is an important tool for carrying out the programs and activities of AMS. These resources provide for quick and efficient communication and access to a wealth of useful information. Under this policy, AMS employees have certain privileges and responsibilities. By authorizing limited personal use of Government office equipment, AMS regards its employees as responsible individuals, capable of balancing this privilege with Agency expectations.

B. This policy does not supersede any other applicable law or regulation. Authorities related to this policy are listed in Section IV, below.

IV. AUTHORITIES

A. Departmental Regulation 3300-1, Telecommunications & Internet Services and Use, dated 3/23/99.

B. Title 5, Code of Federal Regulations (CFR), Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

C. Title 41 CFR, section 101-35.201, Authorized use of long distance telephone services.

D. Executive Order 13011, Federal information technology.

E. *-Federal Information Security Management Act (FISMA), 2002-*

V. DEFINITIONS

A. Government office equipment includes, but is not limited to: personal computers, related equipment and software, Internet services, e-mail, library resources, telephones, facsimile machines, photocopiers and office supplies.

B. Minimal additional expense means the expense incurred when the Government is already providing equipment, supplies or services and you use only limited additional amounts of electricity, ink, toner or paper. Wear and tear from normal use is also considered minimal additional expense.

C. Non-work time means the time when you are not performing an activity for the benefit of the Agency and under the control or direction of the Agency. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after your normal workday, or weekends and holidays.

D. Personal use means uses other than official Government business. *- Use of Government equipment for negotiated grievances or other union business shall be considered personal use and subject to the provisions herein except to the extent that agreements between the Agency and the unions specify otherwise. Personal use policy is the same whether the Government equipment is used in the Government office or in a work at home (or other off site) environment. -*

E. Privilege means that you have no inherent right to personal use of Government office equipment.

VI. POLICY

A. Generally, AMS employees may use Government office equipment for official purposes only. However, limited personal use is allowed in accordance with the following restrictions:

1. Limited personal use is authorized only if it involves minimal additional expense to the Government.
2. Limited personal use is authorized only during non-work time.
3. Limited personal use must not reduce your productivity or interfere with your official duties or the official duties of others.
4. Before limited personal use is authorized, the equipment must be available to you for official Government business. Furthermore, AMS is not required to supply you with equipment if it is not required for you to perform official Government business.
5. Managers and supervisors may further restrict personal use based on the needs of the office or problems with inappropriate use in the office. In such cases affecting bargaining unit employees, the unions will be notified.

B. AMS employees **may not**:

1. Use Government office equipment for personal commercial purposes or in support of other external enterprises such as outside employment or businesses (e.g., selling real estate, preparing tax returns, trading stock).

2. View, download, store, transmit or copy materials that are sexually explicit or sexually oriented, related to gambling, illegal weapons, terrorist activities or any other prohibited activities.
3. Use Government office equipment to engage in any outside fund raising activity, endorse any product or service, or participate in lobbying or prohibited partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).
4. Create, copy or transmit any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation.
5. Create, copy or transmit chain letters or other mass mailings, regardless of the subject matter.
6. *-Use public instant messaging (IM) services such as AOL or Yahoo on a Government computer unless the use of the service has been approved by the Agency as an accommodation.-*
7. Use large files while engaging in limited personal use of Government equipment. For example, sending or receiving greeting cards, video, sound, interactive games or other large file attachments may hinder the performance of an entire network. You should not subscribe to Internet services that automatically download *-personal information-*, such as sports scores, stock prices, or other continuous data streams, such as music or videos.
8. Load personal software onto your computer or make *-unauthorized software or hardware-* configuration changes. For example, computer games and personal tax programs may not be loaded on Agency computers.
9. Use Government equipment as a staging ground or platform to gain unauthorized access to other systems.
10. Acquire, reproduce, transmit, distribute or use any controlled information including computer software and data protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.
11. *-Use or install any Peer to Peer (P2P) file sharing applications, such as Kazaa, Napster, Gnutella, and other P2P applications.-*
12. *-Connect personally owned computer systems to any Government-owned networks or telecommunications equipment; without prior approval from your supervisor and the Agency Chief Information Officer (CIO)-*
13. Make personal long distance telephone calls. However, there are three exceptions:
 - a. In an emergency,
 - b. Brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor), or
 - c. Brief calls home within the local commuting area (e.g., to arrange transportation, check on a sick child).

C. If you ever receive any prohibited material from someone else, you must reply to that person that the material is inappropriate and that the sender must not send this type of material to you again. You must also notify your supervisor; supervisors must exercise judgment, depending on the nature and offensiveness of the material, whether to refer the matter to the Compliance Office, Employee and Management Relations, and/or the Civil Rights Program for action.

D. You must ensure that your personal use does not give the appearance that you are acting in an official capacity. For example, you may not post AMS information to external news groups, bulletin boards or other public forums without AMS authorization. Further, you must not give the appearance that AMS endorses or sanctions your personal activities. If your actions leave the impression that your personal activities are endorsed by AMS, you may be in violation of the standards of ethical conduct for executive branch employees.

If there is any potential for confusion, you should provide an appropriate disclaimer. Here is an example of a disclaimer: "The content of this message is mine personally and does not reflect any position of the Government or of AMS."

E. These restrictions apply to all AMS employees regardless of duty location. For example, if you are a grader performing duties in a processing plant where a computer has been provided to you by either the plant or AMS for your use, or if you are co-located with State department of agriculture employees, the restrictions still apply.

F. Contractors are not authorized limited personal use of Government office equipment, unless it is specifically permitted by contract or other memorandum of agreement.

VII. PRIVACY

A. You do not have the right to privacy while using any Government office equipment, including Internet or e-mail services. Furthermore, your use of Government office equipment, for whatever purpose, is not secure, private or anonymous. While using Government office equipment, your use may be monitored or recorded. If Government office equipment or services are involved at any point in the creation, transmission, or receipt of personal information, then this policy applies and your use may be monitored. For example, if you use a Government PC to read or respond to personal e-mail sent to you at a non-Government e-mail address (e.g., AOL, Yahoo), your use may be monitored.

B. Official telephone calls may be monitored or recorded for legitimate business purposes such as providing training, instruction or protection against abusive calls. Any such monitoring must be in accordance with Federal statutes governing Wiretapping, Investigative Monitoring and Eavesdropping Activity (WIMEA).

VIII. PENALTIES

Unauthorized or inappropriate use of Government office equipment may result in the loss or limitation of your privilege. You may also face administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

IX. SECURITY

A. *-A security breach on one AMS computer can potentially compromise the entire AMS network. As long as the AMS computers are attached to the Internet, they are at risk and will be attacked. We must all take the necessary precautions to defend against these attacks. If everyone does their job in

protecting our AMS information assets, we will be less vulnerable to these attacks. Attacks can range in severity from being a nuisance to a complete shutdown of the AMS network, leading to a significant loss in productivity, time, and money.-*

If you are using Government office equipment, particularly computer systems, you share the responsibility for protecting the security of this equipment with all other users. You must be aware of and follow appropriate security provisions concerning logging on or off Agency computer systems and networks. You are responsible for maintaining the confidentiality of your *-network ID and other Agency-issued passwords,-* and for *-protecting and preserving business information that you place on an Agency computer.-* Because most Agency computers and systems are protected from unauthorized users by passwords, it is particularly critical that you not divulge your passwords to anyone.

B. You should report all security breaches, including compromised passwords, to your supervisor, and/or program security point of contact.

X. QUESTIONS

If you have any questions concerning use of Government office equipment, contact the Information Technology Group (ITG), Science and Technology Program, or the Compliance Office, Compliance & Analysis Program, AMS.

/s/

Lloyd C. Day
Administrator