Department of Homeland Security
Management Directives System
MD Number: 4600.1
Issue Date: 04/14/2003

PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT

I. Purpose

This directive provides Department of Homeland Security (DHS) policy regarding personal use of government office equipment.

II. Scope

This directive applies to all DHS organizational elements.

III. Authorities

This directive is governed by numerous Executive Orders (E.O.) and regulations, such as:

A. E.O. 12674/12731

B. E.O. 13011

C. 5 CFR, Part 2635

IV. Definitions

A. ***Government office equipment***: Equipment and systems purchased and/or owned by the government. Includes, but is not limited to, information technology equipment, pagers, Internet services, email, library resources, telephones, facsimile machines, photocopiers, and office supplies.

B. ***Personal use***: Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization.

C. ***Information technology***: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes, but is not limited to, desktop computers, personal computers, laptops, handheld computers, Personal Digital Assistants (PDAs), related peripheral equipment, and software.

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

E. ***Non-work time***: The time when DHS users are not performing an activity for the benefit of the Department and under the control or direction of the Department. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after a workday, weekends or holidays, but only if your duty station would normally be available to you at such times.

V. Responsibilities

A. The ***Under Secretary for Management***, through the DHS Chief Information Officer (CIO), is responsible for all aspects of this directive, including:

1. Issuing and updating policy on the personal use of office equipment within DHS.

2. Ensuring employees receive Awareness Training on the policy.

B. ***Organizational Element Heads*** are responsible for:

1. Providing all employees with a copy of this directive.

2. Ensuring proper understanding of the directive.

3. Taking appropriate actions when notified of non-compliance with the directive.

C. ***DHS Employees*** using Government office equipment, particularly computer systems, must:

1. Share the responsibility for protecting the security of this equipment with all other users.

2. Be aware of and follow appropriate security provisions concerning logging on or off DHS computer systems and networks.

3. Maintain the confidentiality of their password and of all data that is placed on or deleted from a DHS computer. It is particularly critical that employees not divulge their passwords to anyone.

4. Report all security breaches, including compromised passwords, to their supervisor.

D. ***DHS employees who telecommute*** must adhere to this directive (in addition to the guidelines provided in the department's telecommuting directive) when telecommuting.

E. ***Contractors, interns, or other users*** of DHS government equipment must refer to the terms, and conditions of their contract or memorandum of agreement.

VI. Policy and Procedures

A. Limited personal use of DHS office equipment is a privilege, not a right. Users have no inherent right to personal use of Government office equipment. DHS is extending the opportunity to its employees to use government property for personal use in an effort to create a more supportive work environment. However, this policy does not create a right to use government office equipment for non-government purposes; nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes.

B. DHS employees may use Government office equipment for authorized purposes only. As set forth below, limited personal use of the government office equipment by employees during non-work time is considered to be an "authorized use" of Government property, when such use:

1. Involves minimal additional expense to the government.

2. Is performed on the employee's non-work time.

3. Does not reduce productivity or interfere with the mission or operations of DHS organizational elements.

4. Does not violate the Standards of Ethical Conduct for Employees of the Executive Branch.

C. ***Authorizations***.

1. Employees must be authorized to use equipment for official Government business before it is available for limited personal use.

2. DHS is not required to supply equipment if that equipment is not required to perform official Government business.

3. Managers and supervisors may further restrict personal use based on the needs of the office or problems with inappropriate use.

D. ***Privacy Expectations***.

Employees do not have any right to nor expectation of privacy while using any Government office equipment, including Internet or email services. Furthermore, use of Government office equipment, for whatever purpose, is not secure, private, or anonymous. While using Government office equipment, employee use may be monitored or recorded. If Government office equipment or services are involved at any point in the transmission or receipt of personal information, then this policy applies and use may be monitored.

E. ***Telephone Calls***.

Business telephone calls may be monitored or recorded for legitimate business purposes such as providing training, instruction or protection against abusive calls. Personal phone conversations and business telephone calls will not be routinely monitored. Before DHS institutes a policy to routinely monitor employees' personal or business phone conversations, employees will be notified.

F. ***Proper Representation***.

1. DHS employees must ensure that personal use does not give the appearance of acting in an official capacity. For example, DHS employees may not post DHS information to external news groups, bulletin boards, or other public forums without DHS authorization.

2. DHS employees must not give the appearance that DHS endorses or sanctions personal activities. If an employee's actions leave the impression that his/her personal activities are endorsed by DHS, the employee may be in violation of the Standards of Ethical Conduct for Executive Branch Employees.

3. DHS employees must make every effort to avoid the potential for confusion. If there is any potential for confusion, employees must provide an appropriate disclaimer, such as:

"The content of this message is mine personally and does not reflect any position of the Government or of DHS."

G. ***Inappropriate Personal Uses***.

1. Using large files - For example, sending or receiving greeting cards, video, sound, interactive games, or other large file attachments may hinder the performance of an entire network or reduce the effectiveness of a DHS system. Employees must not subscribe to Internet services that automatically download information (e.g., sports scores, stock prices or other continuous data streams).

2. Loading personal software onto a government computer or making configuration changes - For example, computer games, personal tax programs and personal schedulers may not be loaded on DHS computers.

3. Making personal long distance telephone calls - 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).

   c. Brief calls home within the local commuting area (e.g., to arrange transportation, check on a sick child).

4. Using Government equipment as a staging ground or platform to gain unauthorized access to other systems.

5. Creating, copying, or transmitting chain letters or other mass mailings, regardless of the subject matter.

6. Creating, copying, or transmitting 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.

7. Viewing, downloading, storing, transmitting or copying materials that are sexually explicit or sexually oriented, related to gambling, illegal weapons, terrorist activities, or any other prohibited activities.

8. Using Government office equipment for commercial purposes or in support of other "for profit" activities such as outside employment or businesses (e.g., selling real estate, preparing tax returns for a fee).

9. Engaging in any outside fund raising activity, endorsing any product or service, or participating in lobbying or prohibited partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).

10. Acquiring, reproducing, transmitting, distributing, or using 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.

H. ***Sanctions for Misuse of Government Equipment***.

Unauthorized or inappropriate use of Government office equipment may result in the loss or limitation of an employee's privilege of limited personal use. Employees 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. The DHS Chief Human Capital Officer will develop policies and procedures to address appropriate discipline for violations.

I. ***Contractors***.

Contractors or other individuals using DHS equipment are not authorized limited personal use of Government office equipment, unless it is specifically permitted by contract or other memoranda of agreement. When authorized, the provisions of this directive shall apply to contractors or other individuals using Government office equipment.

J. ***Questions or Concerns***: Any questions or concerns regarding this directive should be addressed to the Office of the DHS Chief Information Officer.