

DEPARTMENT OF HEALTH AND HUMAN SERVICES
PUBLIC HEALTH SERVICE INDIAN HEALTH SERVICE
Rockville, Maryland 20857

Refer to OMS/DIR

INDIAN HEALTH SERVICE CIRCULAR NO. 2001-04

LIMITED PERSONAL USE OF INFORMATION TECHNOLOGY RESOURCES

Sec.

1. Purpose
2. Background
3. Policy
4. Scope
5. Roles and Responsibilities
6. Applicable Laws/Guidance
7. Definitions
8. Prohibited Use of IHS IT Resources
9. Specific Provisions on Use of IT Resources
10. Misuse or Inappropriate Personal Uses
11. Proper Representation
12. Access Management
13. Privacy Expectations
14. Implied Consent
15. Monitoring Tools
16. Penalties
17. Labor Relations
18. Supersedure
19. Effective Date

1. PURPOSE. The purpose of this circular is to establish the Indian Health Service (IHS) policy for limited acceptable personal use of Agency owned information technology (IT) resources by IHS staff and contract personnel. Indian Health Service employees may use IHS IT resources for non-government purposes when such use involves minimal additional expense to the Government, is performed on the employee's non-work time, does not interfere with the mission, or operations of IHS, and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch. This circular supplements the "Department of Health and Human Services (HHS) Information Resources Management (IRM) Policy for Personal Use of Information Technology Resources" approved on January 8, 2001, as amended.

2. BACKGROUND. The IHS serves the American Indian and Alaska Native (AI/AN) people through hundreds of employees located in offices across the nation. The IHS is called upon to deliver more and better services to a growing population that continues to expect increasing improvements in service delivery. Much of this productivity increase has resulted from the use of modern IT such as computers, facsimile machines, and the Internet. This technology raises new opportunities for employees and enables them to perform their jobs more efficiently.

Taxpayers expect to receive maximum benefit for their tax dollars and they depend on the IHS to manage their tax dollars wisely and effectively. The productiveness of IHS is increased when members of the public are confident that their government is well-managed and assets are used appropriately. The relationship between the Executive Branch and the employees who administer the functions of the IHS is one based on trust. Consequently, employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct. The Standards of Conduct for Employees of the Executive Branch, (Section 2635.101 (b)(5)) state, "Employees shall put forth honest effort in the performance of their duties." The IHS believes that employees should be provided with a professional and supportive work environment that includes the appropriate tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps IHS to retain highly qualified and skilled workers.

3. POLICY. It is the policy of the IHS to permit, at the discretion of management, all IHS employees limited use of IHS IT resources for personal needs provided it does not interfere with official business and involves minimal additional expense to the Government. The limited personal use of IHS IT resources must occur during the employee's non-work time, without exception. This privilege to use IHS IT resources for non-government purposes may be revoked or limited at any time by appropriate IHS or HHS officials. This circular does not limit IHS personnel in the use of IHS-owned IT resources for official activities.
4. SCOPE. This circular applies to all IHS organizational components including, but not limited to, Headquarters, Area Offices, and Service Units conducting business for and on behalf of the IHS through contractual relationships when using IHS IT resources. The policies contained in this circular apply to all IHS IT activities including the equipment, procedures, and technologies that are

employed in managing these activities. The policy includes teleworking, travel, other off-site locations, and all IHS office locations. Agency officials shall apply this policy to contractor personnel, interns, externs, and other non-government employees by incorporating such reference in contracts or memorandums of agreement as conditions for using government provided IT resources.

5. ROLES AND RESPONSIBILITIES.

A. Chief Information Officer. The IHS Chief Information Officer (CIO) is responsible for:

- (1) Disseminating this policy to all employees within the IHS.
- (2) Developing and maintaining the IHS personal use policy.

B. Management Officials. The IHS management officials, in their supervisory roles, are responsible for:

- (1) Informing users of their rights and responsibilities, including the dissemination of the information in this circular to individual users.
- (2) Addressing inappropriate use by employees who report to them.
- (3) Receiving reports of inappropriate use from IT resource management officials and sharing these reports, as appropriate, within their own management structure.
- (4) Notifying law enforcement officials when misuse involves committing a crime.
- (5) Managers of IHS IT resources may use system monitoring software to improve the performance of the resource (See Section 15 Monitoring Tools). When a management official identifies an inappropriate use, he/she shall notify the IHS CIO through the normal chain of command and, as appropriate, terminate the individual's access to the IT resource after informing the IHS CIO of the action to be taken.
- (6) Management officials may further restrict their organization's personal use of IHS IT resources within their areas of responsibility.

C. Users of IHS IT Resources. Users, including IHS employees and contractors, are responsible for:

- (1) Seeking guidance from their supervisors when in doubt about the implementation of this policy.
- (2) Following policies and procedures in their use of IHS IT resources and refraining from any practices that might jeopardize IHS computer systems and data files, including but not limited to, virus attacks when downloading files from the Internet.
- (3) 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 (e.g., Internet Engineering Task Force, Request for Comments - Number 1780).
- (4) Familiarizing themselves with any special requirements for accessing, protecting and using data, including Privacy Act requirements, copyright requirements, and procurement sensitive data.
- (5) Adhering to all conditions set forth in this circular.

6. APPLICABLE LAWS/GUIDANCE. Generally, IHS employees may use IHS IT resources for authorized purposes only. As set forth below, limited personal use of IHS IT resources by employees during non-work time is considered to be an "authorized use" of Government property. The "HHS IRM Policy for Personal Use of Information Technology Resources" approved on January 8, 2001, as amended, authorizes HHS operating divisions to adopt policies on personal use of IT resources. Title 5 United States Code (U.S.C.), Section 301, provides that the head of an executive department or military department may prescribe regulations for the use of its property. Also, Executive Order 13011, "Federal Information Technology," Section 3 (a) (1), delineates the responsibilities of the Federal Chief Information Officer Council by providing recommendations to agency heads relating to the management and use of IT resources. Other authorities include:

- A. Computer Security Act of 1987, Public Law (P.L.) 100-235, 101 Stat. 1724

- B. The Privacy Act
- C. The Hatch Act (Standards of Conduct)
- D. The Freedom of Information Act (FOIA)
- E. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources"
- F. "Standards of Ethical Conduct for Employees of the Executive Branch" promulgated by the Office of Government Ethics
- G. Internet Engineering Task Force, Request for Comments Number 1780, J. Postel, "Internet Official Protocol Standards," March 28, 1995 The IHS policies contained in this circular shall also be exercised in accordance with P.L. 93-638, the Indian Self-Determination and Education Assistance Act, as amended, and the Secretary, HHS, policy statement dated August 7, 1997, as amended, entitled "Department Policy on Consultation with American Indian/Alaska Native Tribes and Indian Organizations." It is IHS policy to consult with Indian people to the greatest practicable extent and to the extent permitted by law before taking actions that affect these people and their tribal governments; to assess the impact of the IHS plans, projects, programs, and activities on tribal and other available resources; and to remove any procedural impediments to working directly with tribal governments of Indian people.

7. DEFINITIONS.

- A. Browser. A browser is a software tool used to locate and view data in standardized formats on other computers.
- B. Employee Non-Work Time. Times when the employee is not expected to be conducting official business. Employees may use IHS IT resources for personal use during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).

- C. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, management, manipulation, movement, control, display, switching, interchange, transmission, or reception of data.
- D. Indian Health Service IT Resources. The IHS IT resources include, but are not limited to: personal computers and related peripheral equipment and software, network and web servers, library resources, telephones, facsimile machines, photocopiers, Internet connectivity and access to Internet services, all forms of e-mail and, for the purposes of this policy, office supplies. It does not include data stored in or transported by such resources.
- E. Internet. A worldwide electronic system of computer networks, which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians, and students, as well as the general public.
- F. Minimal Additional Expense. An employee's personal use of IHS IT resources is limited to those situations where the Government is already providing equipment or services and the employee's use of such equipment or services shall not result in any additional expense to the Government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print out a limited number of pages of material, making occasional brief personal phone calls (within IHS policy and 41 CFR 101-35.201, which states that an employee may make a personal long distance call charged to his/her personal calling card), infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.
- G. Personal Use. Personal use means any activity that is conducted for purposes other than accomplishing official or government business. This includes use by employees on behalf of professional organizations or associations.
- H. Privilege. The IHS is extending the opportunity to its employees to use IHS IT resources for personal use in an effort to create a more supportive work environment. This circular does not create the right to use IHS IT resources

for non-government purposes and does not extend the privilege to modifying such equipment, including loading personal software or making configuration changes.

- I. Shared IHS IT Resource. Any IHS IT resource that is managed by one IHS organization but used by many (e.g., the IHS homepage).
 - J. World-Wide Web. A collection of web pages (documents), which are developed in accordance with the Hyper Text Markup Language Web format standard and may be accessed via Internet connections using a WWW browser.
8. PROHIBITED USE OF IHS IT RESOURCES. Employees are specifically prohibited from using IHS IT resources to maintain or support a personal private business. Examples of this prohibition include: employees using a government computer and Internet connection to run a consultant business, travel service, or investment service. The ban on using IHS IT resources to support a personal private business also includes employees using IHS IT resources to assist relatives, friends, or other persons in such activities. However, employees may, for example, make limited use of IHS IT resources to check their Thrift Savings Plan or other personal investments, or to seek employment or communicate with a volunteer charity organization.
9. SPECIFIC PROVISIONS ON USE OF IT RESOURCES. Employees are authorized limited personal use of IHS IT resources. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the Government in areas such as:
- A. Communications infrastructure costs, e.g., telephone charges (personal long distance calls are to be charged to the employee's personal calling card), telecommunications traffic, etc.
 - B. Use of consumables in limited amounts, e.g., paper, ink, toner, etc.
 - C. General wear and tear on equipment.
 - D. Data storage on storage devices.

E. Transmission impacts with moderate e-mail message sizes, such as, e-mails with small attachments.

10. MISUSE OR INAPPROPRIATE PERSONAL USES. Employees are expected to conduct themselves professionally in the workplace and to refrain from using IHS IT resources for activities that are inappropriate. Misuse or inappropriate personal use of IHS IT resources include:

A. Congestion, Delay, or Disruption of Service. Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use.

B. Sexually Explicit or Sexually Oriented Materials. The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials for personal use.

C. Illegal Gambling/Weapons/Activities, Terrorist Activities, or Activities Otherwise Prohibited. The intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.

D. Commercial Purposes, "For-Profit" Activities, or Business Activity. Use for commercial purposes, in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

E. Outside Fund-Raising Activity, Endorsing, Lobbying, or Prohibited Partisan Political Activity. Engaging in any outside fund-raising activity including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

- F. Posting IHS Information Without Authority. Posting IHS or personal information to external news groups, bulletin boards, or other public forums without authority, including information that is at odds with the IHS mission or positions. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate IHS approval has been obtained.
- G. Web Pages. Any use that establishes personal, commercial, and/or non-profit organizational web pages on IHS-owned machines.
- H. Unauthorized Access. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
- I. Chain Letters or Other Unauthorized Mass Mailings. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- J. Illegal, Inappropriate, or Offensive Use. Using IHS IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech or material that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- K. Addition of Personal IT Resources. The addition of personal IT resources to existing IHS IT resources without the appropriate management authorization, including the installation of modems on IHS data lines and reconfiguration of systems.
- L. Additional Expense. Any use that could generate more than minimal additional expense to the Government.
- M. Transmission, or Distribution of any Controlled Information, Copyrighted, Trademarked or Material With Other Intellectual Property Rights, Proprietary Data, or Export Controlled Software or Data. The intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer

software and data that includes information subject to the Privacy Act, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

- N. Unauthorized List Servers and Newsletters. Use or creation of unauthorized list servers or the distribution of unauthorized newsletters.
 - O. Digital Authentication. Using another person's digital authentication.
 - P. Anonymous Messages. Sending anonymous messages.
 - Q. Security Avoidance. Avoiding established security procedures.
10. PROPER REPRESENTATION. Each employee is responsible for ensuring they do not give the false impression that they are acting in an official capacity when using IHS IT resources for non-government purposes. If there is expectation that such a personal use could be interpreted to represent the IHS, then an adequate disclaimer must be used. One acceptable disclaimer is, "The contents of this message are mine personally and cannot be construed to be endorsed (inferred or implied) by the Government or the IHS."
11. ACCESS MANAGEMENT. Employees have no inherent right to use IHS IT resources for personal use. Therefore, the IHS will establish appropriate management controls to ensure that IHS IT resources are used appropriately.
12. PRIVACY EXPECTATIONS. Any use of IHS IT resources, including e-mail, is made with the understanding that such use may not be secure, is not private, is not anonymous and may be subject to disclosure under the FOIA. Employees do not have a right to, nor shall they have an expectation of, privacy while using IHS IT resources at any time, including accessing the Internet through IHS or HHS gateways and using e-mail, which may be subject to release pursuant to the FOIA. To the extent that employees wish that their private activities remain private, they shall avoid making personal use of IHS IT resources.

The privacy rights of an individual may not be violated.

13. IMPLIED CONSENT. Employees imply their consent to disclosing the contents of any file(s) or information maintained or passed through IHS IT resources. By using IHS IT resources, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet and using e-mail.
14. MONITORING TOOLS. The IHS system managers and supervisors may access any electronic communications and employ monitoring tools to detect improper use. Electronic communications may be disclosed within the IHS to employees who have a need to know in the performance of their duties (e.g., with manager approval, technical staff may employ monitoring tools in order to maximize the use of their resources, which may include the detection of inappropriate use).
16. PENALTIES. Unauthorized or improper use of IHS IT resources could result in the loss of use or limitations on the use of IHS IT resources, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of improper use.
17. LABOR RELATIONS. These policies and procedures will not be implemented in any recognized bargaining unit until the Union is provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

Future labor management agreements shall comply with this circular.
18. SUPERSEDURE. None.
19. EFFECTIVE DATE. This circular is effective upon date of signature.



Michael H. Trujillo, M.D., M.P.H., M.S.
Assistant Surgeon General
Director, Indian Health Service