

USE OF CDC INFORMATION TECHNOLOGY RESOURCES

Sections:	1. PURPOSE AND SCOPE
	2. BACKGROUND
	3. POLICY
	4. RESPONSIBILITIES
	5. REFERENCES
	6. ABBREVIATIONS AND ACRONYMS
	7. DEFINITIONS

1. PURPOSE AND SCOPE

This issuance establishes the policy for use of information technology resources and rules of behavior at the Centers for Disease Control and Prevention (CDC)². This policy applies to all information technology (IT) resources owned by, or operated on behalf of, CDC, regardless of location. This policy does not supersede any other applicable law or higher level agency directive, policy guidance, or existing labor management agreement in effect as of the effective date of this policy.

2. BACKGROUND

The mission of CDC requires its employees and contractors to have access to IT resources to support the conduct of official programmatic, scientific and administrative duties. Use of these resources is intended for official purposes.

3. POLICY

Individuals are authorized by their CDC management or sponsor to use CDC IT resources for the conduct of official duties and for limited personal use. Individuals have no inherent right to employ CDC IT resources, and this authorization may be rescinded on an individual basis.

Use of CDC IT resources is governed by this policy as well as the policies, implementation procedures, and other guidance documents published on the Intranet web sites of the Information Technology Services Office ([ITSO](#)), the Office of the Chief Information Security Officer ([OCISO](#)), Management Analysis and Services Office ([MASO](#)), and other applicable federal laws, regulations, and policies.

¹ Updated to include guidance on storing unencrypted data on mobile devices and portable media (see Section 3.B (1)(c)).

² References to CDC also apply to the Agency for Toxic Substances and Disease Registry (ATSDR).

Employees are permitted *limited personal use* of CDC IT resources in accordance with the [HHS Office of the Chief Information Officer \(OCIO\) Policy for Personal Use of Information Technology Resources](#). Such use must:

- Be incidental.
- Involve minimal additional expense to the government.
- Be performed on the employee's personal time.
- Not interfere with the mission or operations of the agency.
- Not violate applicable law.

Misuses or inappropriate personal uses of CDC IT resources are outlined in the [HHS OCIO Policy for Personal Use of Information Technology Resources](#). Examples of unauthorized uses include:

- Interfering with the operation or availability of CDC IT systems.
- Unauthorized accessing, modifying, destroying, or disclosing information or data contained in systems.
- Using CDC systems as a staging ground or platform to gain unauthorized access to systems.
- Sending anonymous messages.

Employees are also permitted use of CDC IT resources during duty hours for the purposes of career development or professional enhancement, as related to the mission of CDC.

Contractors may be permitted the use of CDC IT resources with written approval from the CDC project officer overseeing the contract. Authorization and scope of contractor use (not to exceed activities permitted by this policy) and disciplinary action for misuse shall be specifically addressed in the contracting document(s).

A. Authority

Government equipment is for official purposes only, or as authorized by the government, per the [HHS OCIO Policy for Personal Use of Information Technology Resources](#) and the regulations cited therein.

OCISO and ITSO may take appropriate action—up to and including the temporary or permanent loss of IT access—should employees not act in accordance with the provisions of this policy.

B. Procedures

This section lists procedures for determining prohibited uses; a list of statutes under which uses are prohibited; privacy expectation; and monitoring, compliance and disciplinary action, if these procedures are violated.

(1) Prohibited Uses

- (a). Use of CDC IT systems and resources are subject to federal laws and regulations governing, including, but not limited to:

- [HHS OCIO Policy for Personal Use of Information Technology Resources](#)
- [Anti-Lobbying Statutes](#)
- [Copyright Act](#)
- [Freedom of Information Act](#)
- Office of Management and Budget ([OMB Circular A-130, Management of Federal Information Resources](#))
- [OMB Memorandum M-04-26, Personal Use Policies and “File Sharing” Technology](#)
- [Privacy Act](#)
- [Standards of Ethical Conduct for Employees of the Executive Branch](#)
- [Trade Secrets Act \(18 United States Code \[U.S.C.\] 1905\)](#)
- [Hatch Act Reform Amendments](#)

(b). With respect to the above listed laws and regulations, prohibited uses include, but are not limited to:

- Lobbying Congress on behalf of causes, individuals, or organizations.
- Promoting or conducting political activities, as defined by the Standards of Ethical Conduct for Employees of the Executive Branch, and governed by the prohibitions against certain political activities ([5 U.S.C. 7321-7326](#), and 18 U.S.C. Sections [602](#), [603](#), [606](#), and [607](#)).
- Accessing or using information that is protected by the Privacy Act, or other federally mandated confidentiality provisions, and/or by OMB Circular A-130, [Management of Federal Information Resources](#), except as permitted by and in compliance with the individual’s official CDC responsibilities.
- Making use of e-mail, Intranet, Internet or other CDC IT resources to advertise, trade (including buying or selling stocks), give away, solicit, or provide goods or services, except under circumstances and conditions that are specifically authorized by CDC (e.g., through SHARE announcements or CDC-sanctioned bulletin boards and list servers). Usage will also conform to the associated sections of General Administration Policy CDC-GA-2004-04, [CDC-GA-2004-04, CDC/ATSDR Employee Organizations and Associations](#).
- Violating copyrights or software licensing agreements.

(c). Individuals, including managers and supervisors, shall not use CDC IT resources or systems in an inappropriate manner that demeans other individuals, groups, or organizations, or causes unnecessary cost, congestion, delay, or disruption of service to any government system or equipment, including:

- Disseminating, intentionally accessing, or storing offensive or disparaging information, including hate literature, pornographic or sexually explicit jokes or images, or racist literature. This restriction does not apply to the conduct of research (including behavioral, scientific, or legal) or to communications, provided that either such exception is authorized in advance and in writing by an individual's parent CDC organization.

- Using hardware and/or software or downloading software to existing CDC IT resources without authorization by ITSO and OCISO, including the installation of modems or wireless devices on CDC data lines and reconfiguration of systems. Wireless devices must be in compliance with Information Security Policy [CDC-IS-2005-01, Wireless Security](#).
- Subscribing to mail lists or listservers that are neither related to official CDC business nor to professional enhancement in support of CDC's mission unless specifically authorized by CDC. This restriction shall include posting or publishing CDC e-mail addresses in electronic forums, printed media, or other places except for official use.
- Using chat services, instant messaging, or other communication services without authorization by ITSO and OCISO.
- Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings, regardless of the subject matter, except as permitted by and in compliance with the [HHS IRM Policy for Use of Broadcast Messages, Spamming and Targeted Audiences](#).
- Conducting or participating in fund or solicitation drives or charitable events not authorized by CDC. (Use of e-mail for authorized charitable events, e.g., Combined Federal Campaign, is permitted).
- Establishing personal, commercial and/or non-profit organizational web sites on government-owned machines.
- Subscribing to “push technology services” that are not related to official CDC business or to professional enhancement. “Push technology services” refer to subscription electronic services that send information to personal computers automatically and routinely as a result of prior registration by the user. Examples of such services include: weather reports, sports news, and stock market updates. Permitted “push technology services” are those that provide information on CDC business or professional enhancement topics such as medical, scientific, health, legal, or technology related subjects.
- Creating, receiving, transmitting, or storing classified (national security) information, except as permitted by and in compliance with Information Resources Management policy [CDC-IR-2002-03: Classified Material](#).
- Using telephones or faxes for long distance personal use, except as may be specifically authorized in Federal travel regulations or other policies.
- Using CDC or organizational logos to misrepresent personal materials as falling under official CDC auspices.
- Intentionally misrepresenting, either implicitly or explicitly, personal views or comments in electronic forums or e-mail as agency policy or position. (Note: if a reasonable person with knowledge of the relevant facts could interpret a personal communication as official business, then a disclaimer shall be used. For

example, "My personal opinion is...", or "While not speaking on behalf of the CDC, I think....")

- Using external e-mail services that bypass the CDC mail server and CDC's Internet virus scanning systems, except as authorized by ITSO and OCISO. Prohibited uses include, but are not limited to, accessing a university or business e-mail account or a personal e-mail account from a commercial service provider.
- Using peer-to-peer file sharing, except for official business use as authorized by ITSO and OCISO.
- Storing unencrypted data on mobile devices and portable media. Mobile devices and portable media must be in compliance with [HHS Encryption Standard for Mobile Devices and Portable Media](#).

In the absence of specific, more restrictive CDC guidance (in any form, including policies, standards, guidelines, or procedures) regarding these issues, compliance with any guidance from HHS is mandatory.

C. Signatures and tag lines

Because CDC IT resources are owned and operated on behalf of the U.S. Government, e-mail messages created by employees and contractors – internally as well as externally (to the public, outside agencies, partner organizations, etc.) – should not contain a signature block, tag line, or auto reply such as an Out of Office message that is a personal expression in nature.

Employee and contractor work-related e-mails shall refrain from adding any personal expressions in their signature block or e-mail tag line. Such personalizations could be perceived to be representations of the agency and, therefore, shall be avoided. Appropriate signature block or tag line information includes:

- Name
- Degrees
- Title
- Organization
- Phone number(s) and other contact information/instructions
- Address and e-mail address
- Links to official Web sites or surveys
- Other official information as directed or approved by a CDC supervisor

E-mail messages sent by an employee or contractor in his/her official capacity should not contain editorial statements, tag lines, photos, personal expressions, or graphics within the signature block that are not related to official business. This direction does not pertain to personal e-mails sent under the "limited personal use" provision of this policy.

D. Privacy Expectation

Any use of CDC IT resources owned by or operated on behalf of the U. S. Government, including e-mail, is made with the understanding that such use might not be secure, is not

private, is not anonymous, and may be subject to disclosure under the Freedom of Information Act (FOIA). Users do not have a right to, nor shall they have any expectation of, privacy, while using government IT resources at any time, including accessing the Internet through government gateways and using e-mail. To the extent that users wish that their private activities remain private, they shall avoid making personal use of government IT resources.

Anything stored, processed, or transmitted using CDC IT resources or other equipment owned by or operated on behalf of the government may be disclosed, without notice, to those who have a need to know in the performance of their duties—which may directly or indirectly lead to the detection of inappropriate use. The need for all such disclosures must be documented in writing (with the basis for the request) by a management official that has authority over the information area and approved in advance by the Chief Information Security Officer (CISO) or the Office of Security and Emergency Preparedness (OSEP) Director. The CISO or the OSEP Director shall submit a copy of the approved written request to the CDC Chief Information Officer in advance of the disclosure—or within 24 hours when advance notice is impractical—and shall maintain a copy of the approved request for at least one year after the expiration of the authorization.

No CDC or contractor staff, including IT administrators, shall take any action to override an individual's system security or enable disclosure of protected information of an individual unless specifically authorized in accordance with the procedures in this section. However, when the individual has left the employment or contractual relationship with CDC, the individual's information assets and system accounts should be reviewed to determine their disposition such as deletion, archiving, or reassignment to other staff. This should be carried out by any appropriate management official in the organization, and IT administrators can be called upon to assist in disposition actions under the direction of the appropriate managerial official.

E. Monitoring, Compliance, and Disciplinary Action

CDC has the capability and the authority to evaluate the performance and use of its IT resources and will routinely monitor their use. Abusing these resources; knowingly interfering with the operation or availability of CDC IT systems; exceeding authorization to access, modify, destroy, disclose, use information or other resources; or otherwise failing to comply with the provisions of this policy may result in disciplinary action and/or financial liability for damages.

4. RESPONSIBILITIES

For the purpose of this policy, the following responsibilities are delineated:

A. CDC Employees, including contractors

- Use during duty hours for the purposes of career development or professional enhancement as related to the mission of CDC.
- Use in accordance with the [HHS OCIO Policy for Personal Use of Information Resources](#) and this policy.

B. OCISO

OCISO has oversight of information security within CDC. OCISO will work with other CDC organizations to control access to CDC databases.

C. Managers and Supervisors

- Oversee the guidelines contained within the policy and standard, and report any improper use of CDC IT resources to OCISO.
- Ensure that contractor authorizations are included in contractor use of CDC IT resources.

5. REFERENCES

- A. Basic Obligation of Public Service, Title [5, Code of Federal Regulations \(C.F.R.\) 2635 Sect. 101 \(2003\)](#). January 1, 2003.
- B. [CDC/ATSDR Employee Organizations and Associations, CDC-GA-2004-04](#). June 30, 2006.
- C. [Classified Material, CDC-IR-2002-03](#). April 2002.
- D. Copyright Act, [17 U.S.C. Sections 102 -110 \(2004\)](#). January 23, 2004.
- E. Disclosure of Confidential Information Generally (Trade Secrets Act), [18 U.S.C. Sect. 93:1905 \(2004\)](#). August 3, 2005.
- F. [Federal Information Security Management Act of 2002 \(FISMA\)](#). December 2002.
- G. Freedom of Information Regulations, HHS, [45 C.F.R. Sect. 5 \(1998\)](#). October 1, 1998.
- H. [Hatch Act Reform Amendments \(political activities\) 5 U.S.C. Chapters 7321-7326 \(2004\)](#). January 8, 2004.
- I. [HHS IRM Policy for Use of Broadcast Messages, Spamming and Targeted Audiences HHS-IRM-2000-0004](#). HHS, January 2001.
- J. [Information Technology Services Office \(ITSO\)](#). Last updated June 2005.
- K. Lobbying With Appropriated Moneys, [18 U.S.C. Sect. 93:1913 \(2004\)](#). August 3, 2005.
- L. [OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources](#). November 28, 2000.
- M. [OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology](#). September 2004.
- N. [Policy for Personal Use of Information Technology Resources HHS-OCIO-2006-0001](#). February 2006.
- O. [Printing Management Manual Guide, Reproduction of Copyrighted Materials](#), CDC-PM-2001-01. December 1997.
- P. Privacy Act Regulations, [45 C.F.R. Sect. 5b \(1998\)](#). October 1, 1998.
- Q. [Standards of Conduct for Employees of the Executive Branch](#). October 2002.
- R. Standards of Ethical Conduct for Employees of the Executive Branch, [5 C.F.R. Part 2635 \(2002\)](#). October 2002.
- S. Soliciting or Making Political Contributions, [18 U.S.C. Chapter 29, Sections 602, 603, 606, and 607](#) (2004). August 3, 2005.
- T. [Office of the Chief Information Security Officer \(OCISO\)](#). Last updated June 2005.
- U. Suitability, Security and Conduct, [5 U.S.C. Sect. 73:7321 \(1993\)](#). January 24, 2002.
- V. Use of Government Property, [5 C.F.R. 2635 Sect. 704 \(2003\)](#). January 1, 2003.
- W. Use of Official Time, [5 C.F.R. 2635 Sect. 705 \(2003\)](#). January 1, 2003.
- X. [Wireless Security, CDC-IS-2005-01](#). March 2005.
- Y. [HHS Encryption Standard for Mobile Devices and Portable Media](#). HHS, August 21, 2007.

6. ABBREVIATIONS AND ACRONYMS

For the purpose of this policy, the following abbreviations and acronyms apply:

- A. **CDC** – Centers for Disease Control and Prevention
- B. **CFR** – Code of Federal Regulations
- C. **CISO** – Chief Information Security Officer
- D. **HHS** – Department of Health and Human Services
- E. **FOIA** – Freedom of Information Act
- F. **IRM** – Information Resources Management
- G. **IT** – information technology
- H. **ITSO** – Information Technology Services Office
- I. **MASO** – Management Analysis and Services Office
- J. **OCIO** – Office of the Chief Information Officer, HHS
- K. **OCISO** – Office of the Chief Information Security Officer
- L. **OSEP** – Office of Security and Emergency Preparedness
- M. **USC** – United States Code

7. DEFINITIONS

For the purpose of this policy, the following definitions apply.

- A. IT resources shall mean information (including electronic data, voice, printed documents, and all other formats) and systems used to store, process, or transmit information (including but not limited to electronic mail, Intranet, Internet, voice mail, telephones, faxes, pagers, and copy/print machines), whether owned by or operated on behalf of CDC, regardless of location (e.g., office, field locations, contractor facilities).
- B. Employee shall refer to personnel employed by the federal government in the following capacities, including, but not limited to: career or career-conditional appointments; guest researchers; temporary appointments, such as students, interns, visiting fellows, volunteers and special volunteers; Commissioned Corps personnel.
- C. Contractor shall refer to a person or business that provides goods or services to the CDC under the terms specified in a contract.