

DHS E-MAIL USAGE

1. Purpose.

This directive establishes Department of Homeland Security (DHS) policy regarding DHS electronic mail (e-mail) usage.

2. Scope.

This directive applies to all DHS organizational elements.

3. Authorities.

This directive is governed by Public Laws, regulations, and other directives, such as:

- A. Computer Fraud and Abuse Act of 1986
- B. Computer Security Act of 1987
- C. Electronic Communications Privacy Act of 1986
- D. Freedom of Information Act
- E. Federal Records Act of 1950
- F. Federal Records Disposal Act
- G. Paperwork Reduction Act of 1995
- H. 5 U.S.C. 552a
- I. 18 U.S.C. 2071
- J. 5 CFR Part 2635
- K. 36 CFR Chapter XII, Subchapter B
- L. DHS MD Number 4300 and Publications, "IT Systems Security"
- M. DHS MD Number 0550, "Records Management", Chapter 2

4. Definitions

A. **Electronic mail (E-mail)**: Information created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, that may be transmitted with the message.

B. **Electronic mail (E-mail) system**: A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on computers, and word processing documents not transmitted on an e-mail system.

- C. **Departmental E-mail Directory**: The e-mail list that contains all DHS e-mail user entries, distribution lists, and special user accounts.
- D. **DHS users**: Individuals authorized to use E-mail as part of their assigned official duties. This includes DHS employees, contractor personnel, and authorized guests using DHS supplied resources.
- E. **Federal Record**: All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. (Federal Records Act, 44 U.S.C. 3101 et seq.)
- F. **Misuse of E-mail**: Any unauthorized, illegal, improper, or inappropriate use of DHS E-mail systems, or any violations of the policies listed herein.
- G. **Recordkeeping system**: A system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.
- H. **System of records**: A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to the individual.

5. Responsibilities.

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

B. **The DHS CIO** is responsible for:

1. Issuing policy and guidelines on the use of e-mail within the DHS.
2. Defining standards (e.g., IMAP, MIME, POP, SMTP, TCP/IP, X.400, X.500, etc.) for DHS e-mail systems to ensure interoperability and interconnectivity.
3. Defining special configurations and processes for Department-wide services, such as the DHS e-mail directory and broadcast messages.
4. Managing and maintaining the DHS Directory Services/E-mail System (DSES), including managing and maintaining anti-virus software for e-mail systems.

C. **DHS users** are responsible for:

1. Reviewing, understanding, and adhering to prescribed DHS e-mail policies and procedures, specifically Chapter 2 of the DHS Records Management, MD-0550;
2. Informing current and potential contacts of the existence of e-mail and of other ways of communicating with DHS;
3. Keeping abreast of records management retention guidelines to ensure all records retention requirements are being met;
4. Consulting upon request with appropriate personnel (e.g., records managers, FOIA officials, Privacy Act officers, security managers, legal staffs, etc.) on e-mail issues;
5. Periodically reviewing saved e-mail messages and promptly deleting all unnecessary messages in accordance with the Department's records management policy; and
6. Adhering to periodic guidelines from the CIO's office regarding individual mail message size (including attachments), total mailbox size limits, and remote access policies, if applicable.

D. **Records Management Officers (RMOs)** are responsible for:

1. Conducting periodic reviews of all electronic mail systems to identify electronic records and ensure the records are scheduled.
2. Establishing a training program for users of electronic mail systems that provides for the management of electronic messages as records.

E. **E-mail Administrators** are responsible for:

1. Ensuring interconnectivity and interoperability with DHS, government, and public e-mail systems;
2. Assigning e-mail addresses that conform with DHS's directory infrastructure;
3. Distributing approved DHS e-mail policies to DHS users;
4. Broadcasting department-wide e-mail messages;
5. Providing awareness training for DHS users on:
 - a) Proper use of electronic mail systems; and
 - b) Appropriate security and privacy measures;
6. Working with the cognizant RMO to ensure proper records retention and disposition requirements for e-mail messages;

7. Developing and implementing audit trails to detect both authorized and unauthorized access and user compliance with DHS e-mail policies and procedures;
8. Implementing and maintaining appropriate security features and controls;
9. Conducting routine tests of e-mail system performance;
10. Testing and documenting the reliability of e-mail systems;
11. Creating and maintaining comprehensive system documentation on all aspects of system design, implementation, maintenance, and oversight; and
12. Ensuring timely termination of e-mail accounts and access privileges of departing DHS users.

F. **Heads of DHS Organizational Elements** are responsible for:

1. Defining proper uses of e-mail beyond those contained in this policy as appropriate.
2. Promoting the use of e-mail in ways that achieve DHS organization strategic/outcome goals and improve service to the public.
3. Sharing new ways to improve performance through the use of e-mail with employees.
4. Enabling e-mail initiatives to be integrated with DHS efforts to re-engineer business processes.
5. Identifying opportunities for improving interactions with other government organizations, industry, academia, and the general public through the use of e-mail.

6. Policy and Procedures

A. Policy

1. E-mail communications will be conducted in a seamless, efficient, and cost effective manner to:
 - a) Increase productivity and information sharing;
 - b) Improve timeliness of service to DHS users and customers;
 - c) Facilitate and strengthen mission and program performance;

d) Provide for the dissemination of public information on a timely basis, on equitable terms; and

e) Enhance the utility of the information to the public and other government entities.

2. DHS e-mail systems will be developed and implemented in a manner that:

a) Enables e-mail communications government wide and with the public;

b) Uses standard protocols;

c) Provides appropriate security;

d) Enables a user-friendly interface;

e) Builds upon existing systems; and

f) Ensures system reliability and integrity.

3. The DHS CIO will specify the DHS standard e-mail server and client applications. Any e-mail upgrade or replacement product that is not consistent with the standard shall have connectors that insure that e-mail delivery, calendar, directory, and workflow shall function seamlessly with the standard.

4. DHS e-mail systems are the property of the federal government. DHS owns the data stored on these e-mail systems, including all e-mail messages, even those deemed personal by their authors.

5. Proper uses of DHS e-mail systems include exchange of information that supports the DHS mission, goals, and objectives, job-related professional development for DHS management and staff, and communications and exchange of information intended to maintain job currency or gain additional knowledge that is directly or indirectly related to job functions.

6. Improper uses of DHS e-mail systems include:

a) Use for any unlawful purpose.

b) Concealment or misrepresentation of names or affiliations in e-mail messages.

c) Unauthorized access, alteration of source or destination addresses of e-mail, or misrepresentation of DHS e-mail systems and the messages contained therein.

d) Initiating actions which interfere with the supervisory or accounting functions of the system, including attempts to obtain "system" privileges.

e) Causing congestion of DHS e-mail systems by such things as the propagation of chain letters, broadcasting inappropriate messages (e.g., unsolicited personal views on social, political, religious, or other non-business matters) to lists or individuals, etc.

f) Use for any commercial purposes, for financial gain, or in support of "for profit" activities.

g) Engaging in any activity that would discredit DHS, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material.

h) Use for posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement and appropriate office approvals have been obtained.

7. E-mail is provided to DHS users for business use. As outlined in DHS IMD-4600, "Personal Use of Government Office Equipment" policy, DHS e-mail systems may be used for limited, **incidental** personal purposes, provided that such use does not:

a) Directly or indirectly interfere with DHS e-mail services;

b) Burden DHS with noticeable incremental cost; or

c) Interfere with DHS user's employment or other obligations to the Government.

8. Standards of ethical conduct and appropriate use apply to the use of DHS e-mail systems.

9. The fact that information is produced or preserved electronically does not confer on it any status that is different from the same information in hard copy.

10. Proper business etiquette should be maintained when communicating via e-mail. When writing e-mail, DHS users should be as clear and concise as possible and avoid remarks, expressions, or attempts at humor that could be misconstrued or misinterpreted. E-mail communications should resemble typical professional/respectful business communications.

11. DHS e-mail systems shall not be used in a manner which infringes upon the intellectual property of others.

B. Procedures

1. E-mail messages determined to be federal records shall be governed by records management federal regulations and DHS MD-0550, "Records Management" directive pertaining to creation, maintenance, adequacy of documentation,

recordkeeping requirements, records management responsibilities, records retention, and records disposition.

(a) E-mail messages are subject to public disclosure in accordance with the Freedom of Information Act (FOIA) and, unless privileged, are subject to discovery in judicial or administrative proceedings.

(b) Privacy

(1) DHS e-mail systems shall not be used to send or receive records subject to the Privacy Act of 1974 without ensuring appropriate security and privacy protection policies and safeguards are in place.

(2) Unauthorized establishment of e-mail systems of records is prohibited.

(3) Privacy Act system(s) of records notice(s) shall be published in the Federal Register for any new system that results from or is related to the use of e-mail.

(4) E-mail, including all messages sent or received on DHS e-mail systems, is subject to monitoring (i.e., communications in process of transmission, records in storage pending receipt, and records in archival storage by or on behalf of the user), by appropriate personnel for business purposes to:

(a) Maintain security of the system;

(b) Carry out records management responsibilities;

(c) Conduct authorized law enforcement surveillance or investigations, including tracking unauthorized access to a DHS e-mail system;

(d) Conduct business during a crisis if an employee is absent when information is required;

(e) Conduct business during a prolonged absence of an employee, when information in the employee's e-mail is required;

(f) Maintain national security; or

(g) Ensure compliance with policy set forth in paragraph 6.A.

2. Security

(a) DHS e-mail systems shall provide for security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information contained in the e-mail system.

(b) DHS e-mail systems that meet the definition of general support system or major application (see Appendix III to OMB Circular A-130-Security of Federal Automated Information Resources) shall have a corresponding system security plan.

(c) Security controls shall be reviewed when modifications are made to DHS e-mail systems.

(d) New or significant changes to DHS e-mail systems that meet the definition of general support system or major application shall not be instituted without the cognizant IT security official ensuring agreement with the applicable security plan.

3. Unauthorized, illegal, improper, or inappropriate use of DHS E-mail systems may result in the loss or limitation of an employee's privilege. Employee's may also face administrative or disciplinary action ranging from counseling to removal from the Department/Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

C. Any questions or concerns regarding this directive should be directed to the Office of the DHS CIO.