

CHAPTER 3

ELECTRONIC MAIL

TABLE OF CONTENTS

3.001	Purpose
3.002	Scope
3.003	References
3.004	Definitions
3.005	Goals
3.006	Policy
3.007	Responsibilities

3.001 Purpose

This chapter establishes policy and responsibilities on the use of electronic mail (e-mail) systems within the Department of Transportation (DOT).

3.002 Scope

This policy applies to all DOT organizations, employees, and contract personnel.

3.003 References

- [Computer Fraud and Abuse Act of 1986](#)
- [Computer Security Act of 1987](#)
- [Electronic Communications Privacy Act of 1986](#)
- [Freedom of Information Act](#)
- [Federal Records Act of 1950](#)
- [Federal Records Disposal Act](#)
- [Paperwork Reduction Act of 1995](#)
- [5 U.S.C. 552a, Privacy Act of 1974](#)
- [18 U.S.C. 2071 "Concealment, Removal, or Mutilation Generally"](#)
- Executive Orders [12674](#) and [12731](#) "Principles of Ethical Conduct of Government Officers and Employees,"
- [5 CFR Part 2635 "Standards of Ethical Conduct for Employees of the Executive Branch"](#)
- [5 CFR Chapter L and 49 CFR Part 99 "Supplemental Standards of Ethical Conduct for Employees of the Department of Transportation"](#)
- [36 CFR Chapter XII, Subchapter B-Records Management](#) of National Archives and Records Administration
- [DOT IT Security Program](#)

3.004 Definitions

- **Departmental organizations** are offices within the Office of the Secretary, operating administrations, offices, divisions, and comparable elements of the DOT.

- **DOT users** are individuals authorized to use e-mail as part of their assigned official duties. This includes DOT employees, contractor personnel, and authorized guests using DOT supplied resources.
- **Electronic mail** is 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.
- **Electronic mail system** is 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.
- **Record** includes 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.)
- **Recordkeeping system** is that in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.
- **System of records** is a collection of 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. Please refer to DIRMM Chapter 8 Privacy Act, for further information.
- **Departmental E-mail Directory** is the list of DOT e-mail addresses, distribution lists, and special user accounts. In Exchange, the Global Address List (GAL) contains the Departmental E-mail Directory via Active Directory.
- **Directory Schema** is the framework consisting of the fields used in the Departmental E-mail Directory.
- **Directory Synchronization** is the bi-directional electronic exchange of e-mail address entries and configuration information between mail servers.
- **Departmental Chief Information Officer (CIO)** is the senior management official responsible for the DOT Electronic Mail.

3.005 Goals

- I. 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 DOT 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.

II. DOT 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.

3.006 Policy

I. General

- A. Microsoft Exchange and Microsoft Outlook are the DOT standard e-mail server and client applications. Any e-mail upgrade or replacement product that is not Exchange or Outlook shall be discouraged. Exceptions must have connectors that insure that e-mail delivery, calendar, directory and workflow shall function seamlessly with Exchange and Outlook.
- B. DOT e-mail systems are the property of the federal government. DOT owns the data stored on these e-mail systems, including all e-mail messages, even those deemed personal by their authors.
- C. Proper uses of DOT e-mail systems include exchange of information that supports the DOT mission, goals, and objectives, job-related professional development for DOT 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.
- D. Improper uses of DOT e-mail systems include:
 - 1. Use for any purpose that violates any laws.

2. Disclosing employee or citizen personal information to an external third party without authorization.
 3. Concealment or misrepresentation of names or affiliations in e-mail messages.
 4. Unauthorized access, alteration of source or destination addresses of e-mail, or misrepresentation of DOT e-mail systems and the messages contained therein.
 5. Initiating actions which interfere with the supervisory or accounting functions of the system, including attempts to obtain "system" privileges.
 6. Causing congestion of DOT 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.
 7. Use for any commercial purposes, for financial gain, or in support of "for profit" activities.
 8. Engaging in any activity that would discredit DOT, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material.
 9. 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.
- E. E-mail is provided to DOT users for business use. DOT e-mail systems may be used for incidental personal purposes provided that such use does not:
1. Directly or indirectly interfere with DOT e-mail services;
 2. Burden DOT with noticeable incremental cost; or
 3. Interfere with DOT user's employment or other obligations to the Government.
- F. Standards of ethical conduct and appropriate use apply to the use of DOT e-mail systems.
- G. 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.
- H. Proper business etiquette should be maintained when communicating via e-mail. When writing e-mail, DOT 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.

II. Records Management

E-mail messages determined to be records shall be managed in accordance with federal regulations pertaining to adequacy of documentation, recordkeeping requirements, records management responsibilities, and records disposition.

III. Access

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.

IV. Privacy

- A. DOT 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.
- B. The establishment of e-mail systems of records must be coordinated through either an OA or Departmental Privacy Officer.
- C. 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.
- D. E-mail, including all messages sent or received on DOT 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:
 - 1. Maintain security of the system;
 - 2. Carry out records management responsibilities;
 - 3. Conduct authorized law enforcement surveillance or investigations, including tracking unauthorized access to a DOT e-mail system;
 - 4. Conduct business during a crisis if an employee is absent when information is required;
 - 5. Conduct business during a prolonged absence of an employee, when information in the employee's e-mail is required;
 - 6. Maintain national security; or
 - 7. Ensure compliance with policy set forth in paragraph 6.a.

V. Security

- A. DOT 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. DOT 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 DOT e-mail systems.
- D. New or significant changes to DOT e-mail systems that meet the definition of general support system or major application shall not be instituted without the appropriate IT security official ensuring agreement with the applicable security plan.

VI. Legal Rights

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

3.007 Responsibilities

Responsibility for the implementation of DOT policies regarding electronic mail policy lies with the following officials. These responsibilities may be delegated as deemed appropriate:

I. The Departmental CIO is responsible for

- A. Issuing policy on the use of e-mail within the DOT.
- B. Defining standards (e.g., IMAP, MIME, POP, SMTP, TCP/IP, X.400, X.500, etc.) for DOT e-mail systems to ensure interoperability and interconnectivity.
- C. Defining special configurations and processes for Department-wide services, such as the DOT e-mail directory and broadcast messages.

II. DOT users are responsible for

- A. Adhering to prescribed DOT e-mail policies and procedures.
- B. Informing current and potential customers of the existence of e-mail and of other ways of communicating with DOT.
- C. Contacting the appropriate Records Management Officer (RMO) to ensure all records retention requirements are being met.
- D. Consulting with appropriate personnel (e.g., records managers, FOIA officials, Privacy Act officers, security managers, legal staffs, etc.) on e-mail issues.

III. Records Management Officers (RMOs) are responsible for

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

IV. E-mail Administrators are responsible for

- A. Ensuring interconnectivity and interoperability with DOT, government, and public e-mail systems.
- B. Assigning e-mail addresses that conform to DOT's directory infrastructure.
- C. Distributing approved DOT e-mail policies to DOT users.
- D. Broadcasting Department-wide e-mail messages.
- E. Providing awareness training for DOT users on:
 - 1. Proper use of electronic mail systems; and
 - 2. Appropriate security measures.
- F. Working with the appropriate RMO to develop records retention and disposition requirements for e-mail messages.
- G. Developing and implementing audit trails to detect both authorized and unauthorized access and user compliance with DOT e-mail policies and procedures.
- H. Implementing and maintaining appropriate security features and controls.
- I. Conducting routine tests of e-mail system performance.
- J. Testing and documenting the reliability of e-mail systems.
- K. Creating and maintaining comprehensive system documentation on all aspects of system design, implementation, maintenance, and oversight.
- L. Ensuring timely termination of e-mail accounts and access privileges of departing DOT users.

V. Heads of Departmental Organizations are responsible for

- A. Defining proper uses of e-mail beyond those contained in this policy as appropriate.
- B. Promoting the use of e-mail in ways that achieve DOT organization strategic/outcome goals and improve service to the public.
- C. Sharing new ways to improve performance through the use of e-mail with employees.
- D. Enabling e-mail initiatives to be integrated with DOT efforts to reengineer business processes.
- E. Identifying opportunities for improving interactions with other government organizations, industry, academia, and the general public through the use of e-mail.