

WEST VIRGINIA DEPARTMENT OF TRANSPORTATION
ADMINISTRATIVE PROCEDURES
VOLUME I, CHAPTER 11

SUBJECT: GENERAL
CHAPTER TITLE: ELECTRONIC MAIL RETENTION

TABLE OF CONTENTS

- I. [INTRODUCTION](#)
- II. [ELECTRONIC MAIL RETENTION POLICIES](#)
 - A. [EMPLOYEES/USERS' RESPONSIBILITIES](#)
 - B. [E-MAIL SYSTEM ADMINISTRATOR'S RESPONSIBILITIES](#)
 - C. [ORGANIZATION MANAGERS' AND SUPERVISORS' RESPONSIBILITIES](#)
- III. [E-MAIL ACCESS AND MONITORING POLICIES](#)
 - A. [ACCESSING OTHER EMPLOYEE'S E-MAIL](#)
 - B. [MONITORING E-MAIL](#)

I. INTRODUCTION

Effective: 12/15/2000

Use of the electronic mail systems (e-mail) is an essential means of daily communications, both internally and externally, to the West Virginia Department of Transportation. Often, e-mail messages include important information relative to a project or business transaction. This information may be received in the body of the e-mail or as an attached file and may serve to provide specific project or work documentation.

In receiving e-mail, employees must carefully consider the content of the message and any attachments and decide as to whether it should be retained (saved). Employees should make the decision to save the information using the same rules as they would if the information were received in paper form. Employees should consult with the immediate supervisor whenever unsure as to the need for retaining an e-mail or attached file.

II. ELECTRONIC MAIL RETENTION POLICIES

Effective: 12/15/2000

A. EMPLOYEE'S/USER'S RESPONSIBILITIES

Employees sending or receiving e-mail must:

1. Ensure that any messages sent or received that are deemed to be departmental transactions or "records" are retained in accordance with established retention policies for like information.
2. Retain e-mail "records" either as a printed copy or as an electronic file.

- a. Store printed e-mail "records" in the relevant subject matter file as would be done with any other printed communication.
 - b. Save electronic e-mail "records" to a storage medium (tape, diskette, hard-drive) on the device (personal computer, server, etc.) as designated by the immediate supervisor.
3. File e-mail "records" and keep them in such a manner as to ensure the copy or file is:
 - a. accessible;
 - b. protected from unauthorized access;
 - c. protected from alteration of any kind;
 - d. and protected from physical damage or loss.
 4. Once retained, the original e-mail must be deleted from the e-mail system.
 5. "Non-record" e-mail should be deleted from the e-mail system regularly.

B. E-MAIL SYSTEM ADMINISTRATOR'S RESPONSIBILITIES

Effective: 9/15/2002

E-Mail System Administrators must:

1. Retain general e-mail back-up files for disaster recovery of the e-mail system. Back-up files and disaster recovery files are for restoring operations in the event of loss or damage to the e-mail system, they are not intended for "record" retention purposes.
2. Keep e-mail back-up files for no more than three weeks. The files (e-mail messages) on the back-up tapes, disks, etc., can be overwritten as a normal practice.
3. E-mail messages on the e-mail server will be kept a maximum of 90 days unless deleted beforehand by the receiver of the message. E-mail messages on the server that are over 90 days old will be automatically deleted.

C. ORGANIZATION MANAGERS' AND SUPERVISORS' RESPONSIBILITIES

Organization managers and supervisors will:

1. Ensure that all employees that receive or send e-mail read and understand these policies as well as any related document retention policies.
2. Prescribe rules, if required, for what kinds of e-mail "records" must be retained as printed copies or must be retained as electronic files.
3. Ensure that appropriate storage medium and storage devices are accessible to employees and ensure that proper security measures are in place including the prevention of alteration of any kind and the prevention of unauthorized access.

III. E-MAIL ACCESS AND MONITORING POLICIES

Effective: 12/15/2000

A. ACCESSING OTHER EMPLOYEE'S E-MAIL

1. Since the use of DOT computers and the computer network are reserved for business use only, no e-mail transmissions/files or their content are restricted from access by authorized personnel.
2. DOT Agency Heads/Commissioners, Division Directors and District Administrators may request access to the e-mail communications of employees in the DOT by contacting the Director of Transportation Human Resources Division.
 - a. All requests must be in writing and signed by the requesting manager.
 - b. All requests must include identification information (author, recipient, date, subject of e-mail needed, etc.) as well as a justification for accessing the e-mail.
 - c. Immediate access, justified by the need to conduct urgent DOT business, may be gained to the e-mail of others by contacting the Director of Transportation Human Resources Division by phone.
3. At the direction of the Director of Transportation Human Resources, the Chief of Information Systems or his/her designees may access and disclose e-mail or files of any employee with just cause, provided that such access and disclosure follows any applicable law, policies and procedures. Just cause includes:
 - a. the need to protect system security,
 - b. the fulfillment of DOT obligations,
 - c. the detection of employee wrongdoing,
 - d. the compliance with legal processes,
 - e. the protection of the rights or property of the DOT.

B. MONITORING E-MAIL

1. Neither the Chief of Information Systems nor members of the Information Services Division will routinely monitor e-mail transmissions or messages. However, these transmissions may be monitored, without prior notification, for the following reasons:
 - a. to protect system security,
 - b. to detect employee wrongdoing,
 - c. to comply with legal processes,
 - d. and to protect the rights or property of the DOT.
2. In the event that e-mail messages observed by the Chief of Information Systems or his/her designee appear to have violated laws, policies or procedures, the evidence will be referred to the proper agency management for appropriate action.
3. DOT Agency Heads/Commissioners, Division Directors and District Administrators may request the monitoring of e-mail communications of subordinates in accordance with the same rules listed in the preceding

"Accessing Other Employee's E-Mail."