

DHHR (Department of Health and Human Resources) Operating Procedure

OP-012 - E-mail

Effective: **Draft: 09/30/02**

3.2 Unacceptable Activities

The following list, although not all-inclusive, provides some examples of unacceptable use of DHHR e-mail. When in doubt, seek authorization from the CIO prior to pursuing the activity.

- 3.2.1 Distribution of "junk" mail such as chain letters, jokes, advertisements, or unauthorized solicitations;
- 3.2.2 Private or personal for-profit activities;
- 3.2.3 Unauthorized not-for-profit business activities. (This includes conducting any non-government-related fund raising or public relations activities such as solicitation for religious and political causes);
- 3.2.4 Unauthorized e-mail message(s) sent for the purpose of promoting real property, goods, or services for sale or lease;
- 3.2.5 Transmission of incendiary statements which might incite violence;
- 3.2.6 Use for, or in support of, unlawful or prohibited activities as defined by Federal, State, and local laws or regulations;
- 3.2.7 Transmission of threatening, offensive, or harassing information (messages or images) which contain defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- 3.2.8 Violation of Federal and State laws dealing with copyrighted materials (including articles and software) or materials protected by a trade secret;
- 3.2.9 Transmission of any information which encourages the use of controlled substances or uses the system for the purpose of criminal intent;
- 3.2.10 Violation of State or DHHR regulations prohibiting sexual harassment;

DHHR (Department of Health and Human Resources) Operating Procedure

OP-012 - E-mail

Effective: **Draft: 09/30/02**

- 3.2.11 Violating the privacy of individual employees by reading their e-mail communications unless specifically authorized to do so;
 - 3.2.12 Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by the e-mail system administrators;
 - 3.2.13 Unauthorized distribution of state data and information; and
 - 3.2.14 Use of personal hardware or software to encrypt any e-mail communication.
- 3.3 Group Messages
- 3.3.1 Group messages or mass mailings are intended for official DHHR use and should be used only for messages of broad interest to the DHHR community.
 - 3.3.1.1 Employees may send a group message to 50 people or less.
 - 3.3.1.2 A single message addressed to more than 50 people must be reviewed and approved by the CIO or a designee.
 - 3.3.1.3 The e-mail systems administrator should be contacted for assistance in developing a group address for mass mailings.
- 3.4 Attachments
- 3.4.1 When sending an e-mail message to one person, attachments should be less than 5 MB in size. (It is estimated that 180 pages of full text equals 1 MB.)
 - 3.4.2 When sending an e-mail message to less than 10 people, the attachment should be less than 2 MB in size.
 - 3.4.3 When sending an e-mail to between 10 and 50 people, the attachment should be less than ½ MB in size.
 - 3.4.4 Use caution when automatically replying to e-mail messages with attachments. Do **NOT** reply to all recipients unless they **ALL** need to see the reply.

DHHR (Department of Health and Human Resources) Operating Procedure

OP-012 - E-mail

Effective: **Draft: 09/30/02**

3.4.5 Delete attachments whenever possible.

3.5 Passwords

3.5.1 To protect the DHHR e-mail system, employees must use secure passwords. The following guidelines apply:

- passwords should be difficult for people or computer programs to guess;
- passwords must not be disclosed to others;
- passwords should be a combination of letters and numbers; and
- passwords must be at least eight characters in length;

3.6 Employee E-Mail Retention Requirements

3.6.1 If e-mail messages are thought to be Departmental transactions (records) they must be collected and maintained - either hard copy or electronic - into a record keeping system, and then deleted from the e-mail messaging system.

3.6.1.1 E-mail records must remain accessible.

3.6.1.2 E-mail records are not required to be stored in their original hardware and software environments, although the original content, structure, and context of the messages need to be maintained.

3.6.1.3 E-mail records must be protected from alteration of any kind.

3.6.2 Informational e-mail messages (non-records) are generally of temporary value and do not need to be collected and maintained into a record keeping system. These messages should be cleared from the e-mail system on a regular basis.

3.6.3 While methods for reviewing, storing, or deleting e-mail messages vary, each employee must comply with the retention standards of the business transaction (records) requirements by doing one of the following:

3.6.3.1 Print the e-mail and store the hard copy in the relevant subject matter file as would be done for any other hard copy communication.

DHHR (Department of Health and Human Resources) Operating Procedure

OP-012 - E-mail

Effective: **Draft: 09/30/02**

3.6.3.2 Electronically store business transactions (records).

3.7 E-mail Systems Administrators Retention Requirements

3.7.1 The e-mail system administrators will retain general back-up files for disaster recovery for the e-mail system for no more than three weeks.

3.7.2 In order to safeguard the integrity of the system and ensure proper functionality, the e-mail administrator retains the right to limit the e-mail retention period to 90 days.

3.8 Authorized Access to E-mail Messages

3.8.1 Any supervisor or manager may **request** access to the e-mail messages of their employees.

3.8.2 Only Bureau Commissioners, Office Directors, and/or the OIG (Office of the Inspector General) have the authority to **approve** requests.

3.8.3 Bureau Commissioners, Office Directors, and/or the OIG must submit a request in writing or e-mail and obtain approval from the CIO. (If the request is in writing, a signature of the requestor and date of the request must be present.)

3.8.4 When approving or denying the request, the CIO must take into consideration the following:

- the ways to minimize the time and effort required to submit and respond to requests;
- the need to minimize interference with DHHR business; and
- the protection of the rights of individuals.

3.8.5 The following information is needed to determine whether a request should be approved:

- Name and title of the person who is requesting to access the information;

DHHR (Department of Health and Human Resources) Operating Procedure

OP-012 - E-mail

Effective: **Draft: 09/30/02**

- Name, e-mail address, and userid of person whose e-mail communications will be accessed;
- Justification for the access request; and
- Required duration and/or time period(s) of the access.

3.8.6 After reviewing all of the information provided, the CIO will approve or deny the request to access the employee's e-mail records.

3.8.7 If approved, the CIO will forward the access request to the Manager of NTS (Network and Technical Support) for processing. Otherwise, all documentation and reason for denial will be returned to the originating Bureau Commissioner or Office Director.

3.8.8 Employees involved in the monitoring activity are obligated to keep all information confidential.

3.8.9 All materials generated by this process will be forwarded to the originating requestor.

4.0 ABUSE/VIOLATIONS

Violation of this OP will subject an individual to disciplinary action ranging from a warning, suspension of privileges, or suspension or dismissal from the DHHR. Depending on the circumstances surrounding the incident, OP violations could result in prosecution under State and Federal statutes.