DOCUMENT: Policy	DOCUMENT NUMBER: 0510	REVISION: Original Revised: 01/02/04	PAGE 1 OF 5
SUBJECT: E-Mail Guidelines and Requirements		EFFECTIVE DATE: September 6, 2000	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy establishes guidelines and minimum requirements governing the acceptable use of, access to, and disclosure of the Department-provided e-mail service.

2.0 SCOPE

This policy applies to any employee who has access to or uses the DHHR (Department of Health and Human Resources) electronic mail services.

3.0 APPLICABLE DOCUMENTS/REQUIREMENTS

3.1 DHHR IT Policy 0501 - Use of IT Resources

3.2 DHHR IT Policy 0502 - Virus Prevention, Detection, and Removal

3.3 DHHR IT Policy 0512 - IT Information Security

3.3 DHHR Operating Procedure 012 - E-mail Guidelines

3.4 DHHR Policy Memorandum 2104 - Progressive Discipline

3.5 DHHR Policy Memorandum 2108 - Employee Conduct

4.0 RESPONSIBILITY/REQUIREMENTS

DHHR's Department-wide e-mail system consists of a network of servers and network devices administered and maintained by MIS personnel. Within this e-mail system, all messages, attachments, files, and folders are automatically encrypted.

4.1 DHHR Responsibility

4.1.1 All Bureaus and/or Offices within DHHR are responsible for the e-mail activities of their employees.

4.1.2 All messages sent or received using these e-mail resources are owned by the DHHR and may be considered Departmental records.

4.1.3 The DHHR reserves the right to monitor and/or log all e-mail communications without notice. **Employees should have no expectation of privacy in the use of the e-mail system.**

4.2 Employee Responsibility (see OP-012)

4.2.1 Employees must use the DHHR e-mail system for all e-mail correspondence.

4.2.2 Only minimal personal use of the DHHR e-mail system is allowed, and should not interfere with the legitimate business of the State.

4.2.3 All e-mail correspondence is considered the property of the DHHR.

4.2.4 Employees must follow specific guidelines when sending mass mailings or group messages.

4.2.5 Employees must be aware of rules regarding e-mail attachments.

4.2.6 Employees must use secure passwords.

4.3 Employee E-mail Retention Requirements (see OP-012)

4.3.1 E-mail messages sent or received in the course of business transactions are DHHR records and must be retained by the employee - in either hard copy or electronic format - for as long as they are needed to meet DHHR requirements.

4.3.2 Informational e-mail messages are non-records. These messages are generally of temporary value and do not need to be collected and maintained into a record keeping system.

4.4 E-mail Systems Administrators Retention Requirements

4.4.1 E-mail system administrators will retain general back-up files for disaster recovery purposes only.

4.4.1.1 Copies of e-mail messages held on back-up systems will remain accessible and may be subject to discovery and monitoring processes.

4.4.2 E-mail messages older than 90 days may be purged from the system.

4.5 Authorized Access to E-mail Messages (see OP-012)

4.5.1 The CIO will not routinely monitor e-mail but may, with prior authorization, access and/or disclose the e-mail or files of an employee with just cause, provided that it follows appropriate procedures designed to assure compliance with DHHR policies. Just cause may include the following:

4.5.1.1 to protect system security;

4.5.1.2 to fulfill DHHR obligations;

4.5.1.3 to detect employee wrongdoing;

4.5.1.4 to comply with legal process; and

4.5.1.5 to protect the rights or property of the DHHR.

4.5.2 Any supervisor or manager may request access to the e-mail messages of their employees. (see OP-012)

4.5.3 If it becomes necessary to access an employee's e-mail to complete urgent DHHR business, Office Directors and/or Bureau Commissioners may request immediate access by contacting the CIO.

4.5.4 The CIO will maintain a file of supporting documentation of all authorized access to e-mail messages.

4.5 Conditions of Disclosure of E-mail Information

4.5.1 The contents of e-mail messages properly obtained for Departmental purposes may

be disclosed within the Department for an official purpose without the permission of the authorized user who created the message.

4.5.2 DHHR will attempt to refrain from disclosure of particular communications if it appears likely to create personal embarrassment, unless such disclosure is required to serve a Departmental purpose or to satisfy a legal obligation.

4.6 Enforcement

4.6.1 The ISO (Information Security Officer) is the person designated by the CIO to monitor and provide initial enforcement of DHHR's information security program and IT policies.

4.6.2 The ISL's (Information Security Liaisons) are employees assigned by the commissioner with each Bureau and/or Office to assist the ISO in the protection of information resources.

4.6.3 The OIG (Office of the Inspector General) is the authority who investigates reported instances of Departmental employee misconduct.

4.7 Violations and Disciplinary Action(s)

4.7.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.7.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the Office Director or Bureau Commissioner for appropriate action.

4.7.3 As determined by the Office Director or the Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.7.4 Anyone who willfully or knowingly violates or otherwise abuses the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Back-up Files - Electronic files created to restore computer system files that have become inaccessible on a computer system.

5.2 Chief Information Officer (CIO) - The director of MIS and the person responsible for all information resources within the DHHR.

5.3 E-mail - Any message sent electronically through one or more computers and/or communications networks, and in most cases has a human originator and receiver.

5.4 E- Mail System - A service that sends messages on computers via local or global networks. E-mail systems provide for storage, and later retrieval of messages and attachments, as well as real-time communication.

5.5 Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy.

5.6 Management Information Services (MIS) - This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.

5.7 Mass Mailings - Information shared with a group of people who need to know the same material, (ex: committee members, individual units within Bureaus, etc.).

5.8 Non-Records - Messages consisting of informational records created primarily for the informal communication of information. These messages are short lived, do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.

5.9 Records - Documentary materials or information, regardless of physical media or characteristics, made or received by an office in connection with the transaction of official business and preserved by that office as evidence of the DHHR's functions, policies, decisions, procedures, operations, or other activities of that office or because of the value of data in the record.

5.10 Retention - Specifies how long the e-mail (sent or received) needs to be kept to satisfy

administrative, legal, fiscal and historical requirements.