

State of Maryland

Department of Health & Mental Hygiene

Parris N. Glendening, Governor *Georges C. Benjamin, M.D., Secretary*

Deputy Secretariat for Operations-Information Resource Management Administration-POLICY 02.01.01
Version Effective December 1, 2001

POLICY ON THE USE OF DHMH ELECTRONIC INFORMATION SYSTEMS

SHORT TITLE: EIS POLICY

I. EXECUTIVE SUMMARY

The Electronic Information System (EIS) Policy is the basic document for guiding employees of the Department of Health and Mental Hygiene (DHMH) in the appropriate use of communications technology for business operations. The policy addresses the DHMH Electronic Information Systems that encompass:

- **Telecommunications** -including telephones, facsimile (fax), and voice mail.
- **Computer systems** -including software, hardware, networks with their storage and communications capacity.
- **Internet and intranet** -including access and use.

The Department's communications with the public need to engender a sense of trust in DHMH and State government. All DHMH employees must be able to work with both electronic and paper-based systems and to handle a variety of data, records, documentation, and information, hereafter referred to generally as information. Regardless of how information is obtained, created, or used during job performance, it must be handled with appropriate security, as established by either (1) DHMH policy; or (2) more restrictive, applicable, federal/state laws, regulations, policies, or procedures.

The EIS Policy is intended to clarify the responsibilities of employees as well as to protect the interests of the Department and health consumers through the appropriate use of information systems. The policy notes that DHMH has a proprietary interest in (1) maintaining the integrity of its State-owned systems, software, related data, information; and (2) controlling the access to and use of its systems, software, and related data/information. It restricts employees from using encryption methods (which could disguise a prohibited use) without formal permission. It further limits the use of these systems for activities that are not business related.

Healthy People in  *Healthy Communities*

DHMH Policies and Procedures Administrator 410 767-5934

Employees are directed to comply with IRMA Data Remanence Protocol requirements. Although files, data, or messages may appear to be "deleted" from the system, employees should be aware that procedures by DHMH to guard against data loss may preserve these items, and such deletion may not ensure confidentiality of the files, data, or messages.

The policy requires that employees abstain from illegal, unethical, or other prohibited use of these systems including fraudulent, harassing, threatening, discriminatory, racist, hate-based, lewd, sexually explicit or otherwise disruptive communications, the playing of electronic computer games, and the request for or sharing of said information inappropriate in the business place.

Additionally, the EIS policy states that communications using electronic mail (e-mail), intranet and internet connections, may be monitored, and employees cannot expect privacy using these means of communications. Employees are required to read the EIS Policy, the Software Copyright Policy, and the Information Assurance Policy, and sign the applicable sections of the Combined Policy Acknowledgment Form. The signed form shall be kept in the employee's DHMH personnel file.

II. BACKGROUND

This policy has been necessitated by the rapidly growing access to and use of e-mail, the internet, and intranet throughout DHMH. Producing, exchanging and retrieving information using electronic information systems presents a valuable opportunity for DHMH and the citizens of Maryland. DHMH recognizes and supports these communication channels and methods as "best business practices", except where more traditional modes of communication would be more appropriate.

Employees are encouraged to use these electronic information systems, but are hereby advised that this use extends important responsibilities to the user. Employees of DHMH are expected to exhibit the same high level of ethical and business standards when using the electronic information systems as they do with the more traditional communication resources, and in their face-to-face business relationships.

This document endeavors to serve the Department's immediate EIS policy needs, and it shall be reviewed and revised in coordination with the Maryland Health Information Coordinating Council (HICC), annually.

III. POLICY STATEMENTS**A. DEFINITIONS**

1. For the purpose of this policy, **employee** shall mean any one who is directly employed by or works for DHMH, whether full-time, part-time, temporary, emergency, contractual, agency, volunteer, or other person who has legal access to DHMH electronic information systems.

2. **Computer** means an electronic, magnetic, optical, or other data processing device or system that performs logical, arithmetic, memory, communications, or information storage, manipulation, and retrieval functions. It includes any data storage or communications facility that is directly related to or operated in conjunction with that device or system.

3. The **internet** can be described as a series of computer networks which provide the combined communication pathways of the telephone, mail, television, and radio. In short, any type of remote communications can be carried out via the internet. The **intranet** is similar to the internet, but can best be described as an "internal Departmental internet" that can only be accessed by authorized users on the local area network (LAN) or wide area network (WAN), or through external arrangements, then referred to as an **extranet**. For the purpose of this policy, internet intranet, or extranet will be considered the same venues, and subsequently referred to as **internet**.

B. GENERAL POLICY

Due to the merging of communications technologies, this policy also addresses, but does not override other more restrictive policies or laws governing the authorized use of telephone, facsimile, and voice mail technologies. Telephones (wired and wireless), facsimile (fax) machines, scanners, computers, computer systems, electronic media equipment (including computer accounts, voicemail, mainframe, midrange, mini, personal and laptop computers, personal digital assistants (PDA's), printers, networks, software, electronic mail or e-mail, internet and World Wide Web access connections, and intranet access and use) in DHMH are provided to DHMH employees for business-related use. Any and all information, as well as the media, database structure, and architecture transmitted by, received from, or stored therein is the property of DHMH. It is the shared responsibility of employees to use these electronic information systems in an efficient, ethical, and lawful manner.

The use of DHMH electronic information systems is a privilege extended by DHMH that may be withdrawn at any time. An employee's use of computer and related information systems may be suspended immediately upon the discovery of a possible violation of these policies and guidelines. Additionally, Personnel actions, up to and including termination, may result.

C. EMPLOYEE ACKNOWLEDGEMENT

Effective with the approval of the DHMH 02.01.06 Information Assurance Policy, all employees are required to complete the applicable sections of the new Combined Policy Acknowledgment Form (Addendum) that acknowledge receipt, review and awareness of IRMA policies, and state that the employee's use of the DHMH electronic information systems constitutes consent to comply with these policies. Annual acknowledgment of the policies will be required, preferably in the presence of the employee's supervisor. Inclusion of the acknowledgement process with the employee's PEP evaluation is suggested.

Technological advances may necessitate policy revisions between annual review cycles, in which case employees with e-mail will be notified electronically, and all others will be notified in writing of such changes. An audit trail that documents receipt of said electronic messages may substitute for an employee's signature when revisions do not coincide with the annual acknowledgment cycle.

D. SPECIFIC EIS POLICY STATEMENTS

1. EIS ARE PROVIDED FOR BUSINESS USE.

Access to EIS resources are provided to DHMH employees for business purposes. Since excessive exchange of messages and files may degrade system speed and efficiency by increasing system traffic and/or taking up memory storage capacity, the use of DHMH electronic information systems for personal purposes, including general announcements, is discouraged and should be limited.

E-mail broadcasts to all DHMH employees result in major system inefficiencies and personnel productivity losses. Employees are specifically prohibited from issuing blanket e-mail broadcasts across the DHMH network unless advance review and approval by a Facility/ Administration /Program Director is obtained. Management is requested

to limit such approvals to messages of an urgent and compelling importance to the Department, where other less immediate forms of communication are not viable.

As an alternative, employees are encouraged to use the DHMH intranet bulletin board, or DHMH "list-servers" where provided to post general information within the Department. Broadcast messages will be monitored. Abuse of electronic information systems privileges may result in disciplinary action up to, and including, termination from State service.

2. NON-BUSINESS USE OF E-MAIL

Fraudulent, harassing, threatening, discriminatory, racist, hate-based, lewd, sexually explicit or otherwise disruptive, inappropriate materials are not to be requested, viewed, transmitted (in any form including encryption or using other deceptive methods), printed, or stored.

"Chain letters," solicitations, and other forms of mass mailings or postings ("spam") are not permitted. As a good business practice, employees should avoid generating, sharing, or replying to non-business related e-mail. Such messages should be deleted. Each employee shall immediately advise his/her supervisor or designee, if inappropriate, harassing, or excessively frivolous, frequent, or erroneous communications are received. If a supervisor is not available, the employee shall contact the Information Resources Management Administration (IRMA) help desk (410 767-6534) for investigation.

3. PASSWORDS

Employees are responsible for protecting their own passwords. Sharing or posting of passwords, user IDs, and account access codes or numbers is not permitted except as noted below. Employees will be held accountable for misuse that occurs through granting such unauthorized access. System generated and other DHMH network passwords are considered to be "on loan," and remain the property of DHMH.

Under "best practice" standards, access to confidential or personal data should be limited, using a need to know protocol; however, each operational unit is responsible for insuring adequate emergency system access. No one person within DHMH should be in the position to use password security to prevent or delay business functions. Refusal by an employee to provide computer system access to a system administrator,

Facility/Administration /Program Director, or other authorized employee under standard operations or emergency conditions may result in disciplinary action up to, and including, termination of employment. See the Information Assurance Policy, DHMH 02.01.06 for more details.

4. MONITORING

DHMH provides electronic information systems for internal and external business communications and data exchange in order to facilitate business operations. Supervisors may monitor telephone utilization, but may not monitor actual telephone conversations, without written pre-approval of the Attorney General.

Although passwords are required for network access, and recommended for e-mail program access, these systems and other protection schemes cannot guarantee confidentiality. E-mail communication and access may be monitored.

5. ENCRYPTION

Confidential information, which has been authorized for transmission, may not be sent by e-mail unless appropriate technology has been used to encrypt the information.

6. AUTHORIZED ENCRYPTION SCHEMES

In order to maintain and assure access to DHMH data, no employee may use an unauthorized encryption scheme. Each program wishing to employ electronic encryption technology to protect stored, confidential, or sensitive data must maintain, in a secure manner, copies of all encryption keys. IRMA will provide technical guidance for the selection of encryption methodologies.

7. DELIBERATE EIS DAMAGE

Deliberately introducing or using software designed to damage, destroy, corrupt, or impede the DHMH electronic information systems with viruses or other harmful effects, is grounds for termination of employment. Moreover, the employee may be subject to personal liability, as well as

civil and criminal penalties that may be provided by law. Employees are required to use DHMH authorized computer-virus detection software when provided.

E. GENERAL INTERNET-INTRANET POLICY STATEMENTS

Even though there is no set of laws regulating the internet, there is an informal code of use called "Netiquette" (Net+Etiquette), which describes what internet users expect from one another while using the internet and World Wide Web. Three primary tenets are:

- (1) Don't break the law;
- (2) Be a good neighbor; and
- (3) Use good judgment.

EIS access accounts are not to be considered personal, private, or confidential. Rather, any mail and/or electronic files identified with an employee account or user ID may be subject to inspection by authorized DHMH personnel.

Internet access originating at DHMH is a privilege, extended by DHMH for business use that may be withdrawn at any time. Internet activity may be monitored. Violations of this policy may result in disciplinary action, up to and including termination from State service.

F. SPECIFIC POLICY STATEMENTS FOR INTERNET USE

When using DHMH internet connections (irrespective of the service provider) the employee is a representative of the State of Maryland, Department of Health and Mental Hygiene, in the internet community. Please be aware of the concerns, dangers, and prohibitions associated with the following actions.

1. IRRESPONSIBLE USE OF EIS RESOURCES

Since capacity of the internal electronic information systems network is limited, large file transfers during peak business hours can compromise the performance of the entire system and deny others equal access. Prior to working with large files (100 megabytes and larger),

please consider the effect on all other DHMH network users. No employee or operational unit of DHMH shall operate an independent internet or intranet server, or a personal computer acting as a server, either on DHMH premises or remotely, to conduct DHMH business unless authorized in writing by the Director, IRMA.

2. USE OF PERSONAL COMPUTER EQUIPMENT

Work may not be performed away from the worksite unless all prevailing and appropriate security and confidentiality policies and laws are strictly followed. In addition, this policy prohibits direct dial-up access to the network or simultaneous dial-up and network connections to those instances where alternatives are not available and written, pre-approval from IRMA has been granted. The exceptions are for the use of GroupWise or other approved e-mail systems.

Personal copies of legally licensed software may be used for business purposes if all of the following conditions are satisfied: 1) The State Software Policy is observed; 2) The license is transferred to DHMH; 3) The supervisor provides written approval; and, 4) The software is installed on State equipment by the authorized system administrator.

3. COPYRIGHT INFRINGEMENT

Actions to obtain, use, modify, store, or distribute proprietary and/or copyrighted software, materials, documents, or other information are to be in accord with State, federal, local, or international law or treaty. This is in accordance with DHMH 02.01.02, Policy on the Use of and Copying of Software and Prevention of Computer Software Copyright Infringement.

(Pursuant to this policy, the combined employee acknowledgment that includes the State of Maryland Software Code of Ethics attestation is attached for employee's signature.) Employees using the internet shall respect all copyright issues regarding software, information, and attributions of authorship. Installing copyrighted software to a DHMH computer without licensing is illegal, and may make the employee liable for copyright infringement. Any employee who has unlicensed or undocumented software on DHMH equipment shall be held accountable for the consequences to the extent of applicable laws and DHMH policy.

4. VIRUS SCANNING AND PROTECTION

Internet users share in the responsibility to protect the network and their equipment from computer viruses and other hostile programs and information. The use of computer-based virus protection software is required. Log-in screen notifications and warnings are required under the Governor's Executive Order 01.01.1983.18 State Data Security Committee. Employees are responsible for reviewing these postings when connecting to the DHMH network and contacting IRMA if further information is required.

5. DAMAGING OR ILLEGAL ACTIVITY

Activity by any DHMH employee that could damage the Department's reputation or potentially place the employee and DHMH at risk for legal proceedings by any party is prohibited. Any actions or statements that are clearly, or could be construed to be misrepresentational, fraudulent, libelous, harassing, discriminatory, racist, hate-based, lewd, sexually explicit, promoting unfair competitive practices, or otherwise disruptive communications are also prohibited. Materials that are inappropriate for the business workplace are not to be requested, viewed, transmitted (in any form, including the use of encryption schemes or use of other deceptive methods), printed, distributed, or stored.

6. HOSTILE ACTIVITY

Actions that may reasonably be construed as hostile by another organization, institution, or individual (internal or external to DHMH) are prohibited. An example of this is attempting to gain unauthorized access to another computer system and/or information.

7. COMMUNICATION CONSTRUED AS AN OFFICIAL DHMH RESPONSE

Posting information on bulletin boards or mailing lists using the DHMH name may be construed as an official DHMH response, and are prohibited without proper authorization. Computer contact people will be

required in all operational unit systems to handle e-mail requests and messages most efficiently, to provide an official response and to work with IRMA. Questions regarding official DHMH responses should be directed to your supervisor, or the DHMH Office of Public Relations.

In addition, employees may not post personal, private, or outside corporate communications of a commercial nature, solicitations, advertisements, or other commercial material using a DHMH associated account.

IV. REFERENCES

- Governor's Executive Order 01.01.1983.18 - State Data Security Committee
- State Agency Information Security Practices, State Data Security Committee
- Article 27, Section 45A and Section 146 of the Annotated Code of Maryland
- Maryland Department of Budget and Fiscal Planning Manual, #95-1, effective date: June 1, 1995, Subject: Prevention of Software Copyright Infringement
- DHMH Policy 02.01.02 (formerly Policy DHMH 9170) -Policy On The Use Of And Copying Of Computer Software And The Prevention Of Computer Software Copyright Infringement, most current version.
- DHMH Policy 02.01.06, Information Assurance Policy (IAP), most current version

V. Addenda

- DHMH Form 4518-Combined IRMA Policy Acknowledgement Form

Approved: 
Georges C. Benjamin, M.D., Secretary

December 1, 2001
Effective Date

COMBINED IRMA POLICY ACKNOWLEDGMENT FORM

This document is a combined policy acknowledgment form for DHMH computer-related policies. Following consultation with your supervisor, please read and initial the appropriate acknowledgment sections, then sign the signature block below.

Acknowledgement Section

Employee Initials	Supervisor Initials °	Policy Number-Statement
		<p>02.01.01 Policy on the Use of DHMH Electronic Information Systems (EIS) I hereby acknowledge awareness of DHMH Policy 02.01.01, and that my use of these systems constitutes my consent to comply with this directive.</p>
		<p>02.01.02-Software Copyright Policy & the State of Maryland Software Code Of Ethics- Unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct. The State disapproves of such copying and recognizes the following principles as a basis for preventing its occurrence.</p> <ol style="list-style-type: none"> 1. The State will not permit the making or using of unauthorized software copies under any circumstances. 2. The State will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs. 3. The State will enforce internal controls to prevent the making or using of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards. <p>I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making copies of, or using unauthorized software may also subject me to civil and criminal penalties. My signature below indicates that I have read and understand Policy 02.01.02- Software Copyright Policy and the State of Maryland Software Code of Ethics.</p>
		<p>02.01.06-Policy to Assure Confidentiality, Integrity and Availability of DHMH Information (IAP) I acknowledge that I am required to comply with the general applicable sections of this policy as it relates to my current job duties. I further acknowledge that should I breach this policy, I am subject to disciplinary, civil, and criminal consequences.</p> <p>.....</p> <p>02.01.06-IAP--"Specific Personnel" Acknowledgement If I am currently designated, or at any time my job duties require me to be designated as a Custodian, Data Steward, Designated Responsible Party, Database Administrator, and/or Network (System) Administrator, I acknowledge that I am required to comply with the corresponding responsibilities assigned to <i>specific personnel</i>. Likewise, if I am currently required, or if at any time my duties include the requirement for preparation or monitoring of contracts or memoranda of understanding, I acknowledge that I am required to comply with the <i>specific personnel</i> provisions of the IAP and guidance.</p>

Employee/User Signature Block

I hereby acknowledge that I have reviewed and understand the above-initialed policies.

Employee/User Signature: _____ DATE: _____

Employee/User Identification (Please Print)

NAME: _____ PIN # or CONTRACT#: _____

AGENCY/COUNTY: _____ ADMINISTRATION/UNIT: _____ LOCATION: _____

Supervisor's Verification

Supervisor Signature: _____ DATE: _____

°Supervisor verifies that the employee/user has acknowledged and initialed the appropriate policies for his/her position.