

# HARFORD COUNTY HEALTH DEPARTMENT POLICY

Title of Policy: Electronic Information Systems and Computer Software Policy	
Program Area: Information Technology	
Approved By: <i>Susan Kelly</i>	Original Effective Date: 12/2001
Susan Kelly, Health Officer	Revised Dates: <i>11/15/13</i>

## 1.0 POLICY

As a unit of the Maryland Department of Health and Mental Hygiene (DHMH), Harford County Health Department (HCHD) follows the DHMH policies on the use of information technology, including:

- a. 02.01.01 Policy on the Use of DHMH Electronic Information Systems (EIS) - Short Title: EIS Policy (Appendix A);
- b. 02.01.02 Policy on the Use and Copying of Software and the Prevention of Computer Software Copyright Infringement (Appendix B); and
- c. 02.01.06 Policy to Assure Confidentiality, Integrity and Availability of DHMH Information – Short Title: Information Assurance Policy - IAP (Appendix C).

Every HCHD staff member and his/her supervisor must sign the “Combined IRMA Policy Acknowledgment Form” (Attachment D), and each employee’s signed form must be kept in his/her personnel file.

## 2.0 PURPOSE

2.1 HCHD communications should engender a sense of trust in government. All HCHD 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.

2.2 The Electronic Information System (EIS) Policy is the basic document for guiding employees of the Harford County Health Department (HCHD) in the appropriate use of communications technology for business operations. The policy addresses:

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

2.3 The Software Copyright policy provides guidance to HCHD employees in the prevention of copyright infringement and use of unauthorized software on HCHD computers. The IAP policy provides direction for certain actions of HCHD employees to assure confidentiality, integrity and availability of HCHD information assets as well as clarifying the roles and responsibilities of employees to protect the interest of HCHD and consumers regarding the release of non-protected information and safeguarding HCHD protected and proprietary information.

### 3.0 PROCEDURES

- 3.1 All HCHD employees are to be provided the three DHMH policies governing information technology (Appendices A, B and C);
- 3.2 All employees must read the policies and sign the acknowledgement form (Appendix D) confirming that they understand the policies prior to being given access to HCHD information services.
- 3.3 All employees will have a copy of the acknowledgement form (Appendix D), signed by the employee, in his/her personnel file.

# DHMH POLICY

<http://dhmh.maryland.gov/SitePages/op02.aspx>

DHMH OFFICE OF INFORMATION TECHNOLOGY -

DHMH POLICY 02.01.01  
Effective Date: October 16, 2013

## EMPLOYEE INFORMATION TECHNOLOGY SECURITY: PROTECTING NON-PUBLIC INFORMATION

### I. EXECUTIVE SUMMARY

The Department of Health and Mental Hygiene (DHMH) takes the protection of private health information very seriously. The privacy and security of DHMH information and information systems is a critical part of normal business practices and is the responsibility of every employee.

All DHMH employees and contractors are responsible for protecting private health information from unauthorized access, modification, disclosure and destruction.

This User Policy provides employees with the basic information needed to understand their role as an IT System user and is based on the DHMH OIT Technical Security Policy, Standards and Requirements, a more detailed and comprehensive document which is available at <http://employeecentral.dhmh.maryland.gov/infosec/pdf/DHMH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf>

### II. BACKGROUND

Information and information technology systems are essential assets of the State of Maryland. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions as well as to other State agencies and to local and federal government entities. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, contractors, and volunteers of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Prior to issuing this policy, DHMH had adopted by reference the IT Security Policy developed by the Maryland Department of Budget and Management. With the recent creation of the Maryland Department of Information Technology and the subsequent publication of IT Security guidance to agencies by DoIT, DHMH, as directed in that policy, developed this policy and its associated standards and requirements. Organizational units within DHMH must use these documents as a guide when procuring information technology and services, service providers, contractors, software, hardware and network components. (References 1, 2 & 3 of this policy)

### III. POLICY STATEMENTS

#### A. DEFINITIONS.

**Department of Health & Mental Hygiene**

OFFICE OF REGULATION AND POLICY COORDINATION (ORPC)  
201 West Preston Street - Suite 512 – Baltimore Maryland 21201-2301  
Phone 410 767-6499 FAX 410 767-6483

For purposes of this policy:

1. **"Employee"** means all agencies, employees, contractors, and volunteers of the State and external users having legal access to State information who are responsible for protecting information from unauthorized access, modification, disclosure and destruction.
2. **"Equipment"** includes workstations, servers, specialized lab diagnostic equipment containing any form of embedded memory, laptops, tablets, portable communication devices, multi-function printers/copiers, and environmental or process control equipment.
3. **"Media"** includes removable media, CDs, magnetic tapes, external hard drives, flash/thumb drives, DVDs, copier hard disk drives, and information system input and output (reports, documents, data files, back-up tapes at the employee's location or those sent offsite).
4. **"Non-Public information"** includes Protected Health Information (PHI), Personally Identifiable Information (PII), and Proprietary Information.
5. **"Public information"** means information that has no restrictions on who can access it.
6. **"Restricted personal use"** means acceptable use that is not job-related.

**B. LABELING.**

Media containing Non-Public information shall be clearly labeled "Confidential." Employees must restrict access to these media containing confidential information to authorized individuals. File names must also reflect that the file is confidential e.g. prefixing CON to the file name "CONclientfiles123.txt."

**C. EMAILING.**

1. Non-Public information must be protected by encryption when sent electronically to others or stored on Google Drive.
2. Using the DHMH Google Government Apps email to send or Google Drive to store Non-Public information is acceptable under the following conditions:
  - a. The user is in another Maryland agency, or is a business associate and has an email address ending in Maryland.gov;
  - b. If storing on Google Drive, or sending to a non Maryland.gov address, the information is contained in a Microsoft Office (Word or Excel) or Adobe "pdf" that has been "locked" with a password (provide password to recipient by telephone); or
  - c. The employee's Maryland.gov email account has been set up with Google Message Encryption and the employee utilizes this service.

(If the employee is unsure whether his or her account has Google Message Encryption, the employee should contact his or her supervisor before sending Non-Public information.)

**D. PHYSICAL TRANSFER OF MEDIA CONTAINING NON-PUBLIC INFORMATION.**

1. Although off-site storage of critical system data is required, it is subject to manager approval.
2. There are stringent controls required for off-site transfer and storage. Details are provided in the full document identified in Reference 2 of this policy.
3. Explicit, written manager authorization is needed before an employee removes backup copies or works with Non-Public information off-site.
4. The use of equipment and media off-site must be reported and registered in accordance with the "Laptop Policy" contained in the full document identified in Reference 2 of this policy.

**E. SECURE ACCESS TO EQUIPMENT AND MEDIA.**

1. Do not allow others to use your log-in credentials.
2. Setup and engage a password required screensaver when leaving workstations.
3. Password-protect cell/smart phones, laptops, tablets, or other devices containing Non-Public information.
4. Securely store or lock down portable equipment to immovable objects (see details on securing laptops contained in the full document identified in Reference 2 of this policy).
5. Make sure all Non-Public information on State-provided storage media is encrypted.
6. Physically secure backup media; all portable storage media such as hard drives, flash media drives, diskettes, magnetic tapes, laptops, PDA devices, DVDs and CDs containing Non-Public information should be locked when unattended.
7. Use only approved remote access methods (contact Network Manager for details). An employee needs their supervisor's permission to work off-site or at home.
8. Wear a State or Federally issued picture employee Identification badge.
9. Ensure visitors are issued and prominently display State issued identification at all times.

10. Accompany visitors to areas containing servers and associated media.

**F. PASSWORD PROTECTION.**

If an employee is authorized to access Non-Public information or agency IT assets, the employee must protect those assets by creating and utilizing strong passwords. Here are a few recommendations:

- Don't send passwords in un-encrypted email messages or other forms of un-protected electronic communication (contact recipient by phone and provide after verifying they are the intended recipient).
- Use at least eight characters.
- Include digits and punctuation characters as well as letters.
- Use both upper and lower case characters.
- Don't use a word in any language, slang, dialect, jargon, etc.
- Don't use personal information, i.e. names of family members, pets, etc.
- Don't discuss passwords with others, write down and post conspicuously, or electronically store unless encrypted.
- Passwords for work, home, and personal accounts MUST be different.
- Don't reveal your personal password over the phone to ANYONE.
- Don't reveal a password on questionnaires or security forms.
- If someone demands a password, have them call the Office of Information Technology (OIT) Help Desk at 410-767-6534.
- Do not use the "Remember Password" feature of applications.
- If it is suspected that an account or password has been compromised, report the incident to OIT HelpDesk 410-767-6534 and change the password immediately.

**G. PERSONAL EQUIPMENT.**

An employee may not use personal devices to store Non-Public information or to conduct State business without written authorization from their supervisor. If approved, there are restricted access rights and security and privacy conditions, including adequate encryption systems, required. Users may access State information resources from home and personal devices if these requirements are met.

**H. WHAT DO I DO WITH EQUIPMENT OR MEDIA I NO LONGER USE OR NEED?**

1. Equipment and Media must be disposed of in an appropriate manner. Data storage devices (hard drives and other data storage devices and media) have to be rendered inoperative, or destroyed or conditioned so data are unrecoverable. Do not throw away used equipment or media; employees should contact their supervisor instead.
2. Disposal of electronic storage media (or printed records) must be in compliance with the employee's Business Unit's detailed document retention policy and all litigation hold procedures. Employees should contact their supervisor or Network Manager for details.

**I. ACCEPTABLE USE OF STATE I.T. RESOURCES.**

1. State I.T. resources are intended for business purposes in serving the interests of the State and the citizens, visitors, and commerce partners of the State of Maryland. All electronic communications created, received, or stored on the State's electronic communications systems are the sole property of the State and **not** the author, recipient, or user unless designated otherwise or protected by prevailing Federal or State law.
2. The following activities are examples of acceptable use of agency electronic communications:
  - Send and receive electronic mail for job related messages, including reports, spreadsheets, maps etc.
  - Use electronic mailing lists and file transfers to expedite official communications within and among State agencies, as well as other job related entities.
  - Access on-line information sources to gather information and knowledge on state and federal legislation, industry best practices, or to obtain specialized information useful to state agencies.
  - Connect with other computer systems to execute job related computer applications, as well as exchange and access datasets.
  - Communicate with vendors to resolve technical problems.

**J. PERSONAL USE OF STATE RESOURCES.**

1. Restricted Personal Use.

The State's electronic communications systems may be used for limited, minor, incidental personal uses, as determined by local management that are not intentional misuses.
2. Personal use is **not** allowed if:

- a. The use directly or indirectly interferes with the Agency's business uses, another user's duties, or burdens the State with more than a negligible cost;
- b. The use violates any provision of this policy, any supplemental policy adopted by DHMH regarding information security and use, electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law; **or**
- c. The employee's manager determines that the employee's personal use exceeds the allowance for minor, incidental, limited use or is otherwise inappropriate.

**K. USER ACCESS TERMINATION.**

An employee's access to State electronic communications systems resources shall cease immediately when one of the following occurs:

1. Termination of employment or consultant's relationship with the State;
2. Leave of absence;
3. Lay-off; or
4. A determination by senior management that an employee's access may constitute a threat to the DHMH network or data infrastructure.

**L. REPORTING SUSPECTED/ACTUAL SECURITY INCIDENTS.**

An information systems security incident is any event, suspected event, or discovery of an action or vulnerability that could pose a threat to the confidentiality, integrity, or availability of supporting systems, applications, or information. An employee must immediately upon discovery report such a concern to their supervisor or management and call the OIT Helpdesk at 410-767-6534.

**M. SANCTIONS FOR POLICY VIOLATION.**

1. DHMH employees must upon employment and annually thereafter sign the "Combined Acknowledgement" form attesting that the employee will follow applicable IT security and copyright policies. (Reference 4 of this policy).
2. Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.
3. Deliberate, unauthorized disclosure of Non-Public information may result in substantial civil and/or criminal penalties.

**N. REQUIRED TRAINING.**



1. OIT has established an extensive on-line awareness and training program which addresses each requirement of this policy and provides links to supplemental State and external IT Security resources which is available at <http://employeecentral.dhmh.maryland.gov/infosec/presentations/InfoSecTraining-MultipleRoles-8-15-2013.pdf>
2. All existing employees who use agency IT resources or have access to Non-Public information must complete this training within 3 months of the issuance of this policy.
3. New employees who use agency IT resources or have access to Non-Public information must complete this training within 14 working days of their employment.

#### **IV. TECHNICAL GUIDANCE / ADDITIONAL INFORMATION.**

##### **A. NEED FURTHER TECHNICAL GUIDANCE?**

Persons with questions or needing further information are encouraged to contact the Director, OIT Security Division, at [david.bickel@maryland.gov](mailto:david.bickel@maryland.gov) or (410-767-5219).

##### **B. LEARN MORE ABOUT IT.**

There are a variety of security resources available to the employee at all times at <http://employeecentral.dhmh.maryland.gov/infosec/index.html> Here the employee can access the detailed security policies, standards, and requirements.

#### **V. REFERENCES**

1. DoIT; various Information Technology security policies, standards and requirements,  
<http://doit.maryland.gov/support/pages/securitypolicies.aspx>
2. DHMH OIT Technical Security Policy, Standards and Requirements  
<http://employeecentral.dhmh.maryland.gov/infosec/pdf/DHMH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf>
3. State Finance and Procurement Article, §3A-403, Annotated Code of Maryland  
<http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gsf&section=3A-403&ext=html&session=2014RS&tab=subject5>
4. Combined OIT Policy Acknowledgement Form  
[http://www.dhmh.maryland.gov/SitePages/sf\\_irma.aspx](http://www.dhmh.maryland.gov/SitePages/sf_irma.aspx)

APPROVED:



---

Joshua M. Sharfstein, M.D., Secretary, DHMH

October 16, 2013  
Effective Date



STATE OF MARYLAND

DHMH

Maryland Department of Health and Mental Hygiene  
201 W. Preston Street • Baltimore, Maryland 21201  
Parris N. Glendening, Governor - Georges C. Benjamin, M.D., Secretary

**DHMH POLICY NUMBER 02.01.02**

**Cross-Reference: Information Resource Management Administration**

**TITLE: POLICY ON THE USE AND COPYING OF SOFTWARE AND THE  
PREVENTION OF COMPUTER SOFTWARE COPYRIGHT INFRINGEMENT**

**I. EXECUTIVE SUMMARY**

This policy states that the Department of Budget and Fiscal Planning (now Department of Budget and Management, DBM) Manual #95-1. Prevention of Software Copyright Infringement, is the basic document for guiding employees of the Department of Health and Mental Hygiene (DHMH) in the prevention of software copyright infringement. **All employees** of the DHMH are told that they shall not make copies of software products or software documentation or use office computers for any purpose other than official business. Software not specifically purchased or acquired through established procurement channels is not authorized for use on DHMH computers. Freeware and/or Shareware products must be reviewed by the Information Technology Support Division before they can be used on any DHMH personal computer (PC), regardless of whether the PC is networked or not. All employees are told that they must sign the **State of Maryland, Software Code of Ethics**.

Specific instructions are given to the Executive Assistant to the Secretary, Deputy Secretaries, Directors of Administration, Superintendents of facilities or equivalent, Local Health Officers, Heads of independent units, and Personnel Officers.

A formal means of control is established to help enforce the policy. A Software Manager position with authority to implement and see to adherence of the software policy is established. The appointment of Software Monitors is mandated and facilities and local health departments are to also have a Chief Software Monitor. The duties of the Software Manager, Chief Software Monitor, and the Software Monitors are enumerated. The date for the submission of the Certification attesting to compliance with State policy for prevention of software copyright Infringement to the Secretary, DBM, by the Secretary, DHMH, is given.

## **II. BACKGROUND**

This **DHMH Policy 02.01.02, Policy On The Use Of And Copying Of Software And The Prevention Of Computer Software Copyright Infringement**, effective May 12, 1998, supersedes and makes obsolete **DHMH Policy 9170, Policy on the Copying of Computer Software**, which was effective 3/17/92.

The Department of Budget and Fiscal Planning (DBFP) on June 1, 1995, promulgated DBFP Manual #95-1. The DBFP Manual #95-1 establishes specific policy and procedure requiring strict adherence to the Federal Copyright Act as regards computer software. The DBFP Manual #95-1 requires the maintaining of adequate software records, the implementing of employee information and control procedures necessary to prevent copyright infringement, and the signing of the State of Maryland Software Code of Ethics by each State employee with known or potential access to a computer or computer software. The DBFP Manual #95-1 also requires that the agency head (Secretary of Health and Mental Hygiene) certify annually that the agency (DHMH) is in compliance with the policies and procedures of the DBFP Manual #95-1.

The added requirements of DBFP Manual #95-1 necessitate issuance of an updated DHMH policy and more comprehensive control, education, and reporting procedures on the part of the Department.

The Copyright Act of 1976, a federal statute, prohibits the making of unauthorized copies of computer software and related documents. Persons who make unauthorized copies are subject to severe civil penalties, even when they are unaware that such conduct is a violation of copyright law. The licenses that come with computer software constitute legally binding agreements whereby the purchasers or users of the software accept automatically (by opening the package) the prohibitions set out therein against making unauthorized copies. Additionally, as it is an established fact that the copying of software is a major cause of computer virus infection and proliferation, the use of only original, licensed software packages will minimize the risk of viral damage to computer systems.

## **III. POLICY STATEMENTS**

### **A. EXCLUSIONS**

This policy does not prohibit the legitimate reproduction of software for archival or back up purposes or for other uses specifically permitted by the software licensor.

**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

**B. DEFINITIONS**

1. **Employee(s)**, for purposes of this policy, shall mean any one who is directly employed by or works for the DHMH whether full time, part-time, temporary, emergency, contractual, agency, or volunteer.
2. **Authorized Software** means software used in accordance with the software license or owned by the agency.
3. **Computer** means an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions. It includes any data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.
4. **Software** means computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.
5. **Department of Health and Mental Hygiene (DHMH)**, for purposes of this policy, shall mean the headquarters, regardless of location; facilities; independent units of the DHMH; and local health departments of each county.

**C. GENERAL**

1. Department of Budget and Fiscal Planning (DBFP) Manual #95-1, Prevention of Software Copyright Infringement, and its attachments is the basic document for guiding employees of DHMH in the prevention of software copyright infringement (See Appendix I).
2. This policy shall augment DBFP Manual #95-1 and give specific instructions to all employees and specific authority to some.
3. The Director, Information Resources Management Administration (IRMA), shall be responsible for the administration and implementation of a program, based on DBFP Manual #95-1 and this policy, to prevent software copyright infringement by employees of the DHMH and train employees of the DHMH regarding software copyright infringement.

**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

4. All Deputy Secretaries or equivalent, Assistant Secretaries or equivalent, Directors of Administrations, Superintendents of facilities or equivalent, Local Health Officers, Heads of independent units, and other managers shall be responsible for periodically informing their employees of this policy and of the pertinent laws and heavy fines to which copyright violators are subject.
5. The Executive Assistant to the Secretary, DHMH, shall:
  - a. Obtain, on or after June 15 of each year but before July 1 of the same year, a memorandum from each Deputy Secretary and the Head of each independent unit certifying that employees under their jurisdiction are in compliance with DBFP Manual #95-1 and this policy.
  - b. Prepare and submit the annual certification which is required by DBM.
6. The appropriate DHMH personnel officer (Director of Personnel Services Administration for Headquarters, Director of Personnel, Personnel Officer, Personnel Associate, etc., for facilities, Independent Units, and Local Health Departments) shall include in the employee's personnel file the original signature copy of the **State of Maryland, Code of Ethics** form of each employee in their jurisdiction who has access to or potential access to computers.
7. Employees of DHMH who have budgetary responsibility and/or supervisory responsibility shall plan for their software needs and shall include sufficient funds in their budgetary requests so that they may provide legally acquired software through the proper channels (See **Policy DHMH 9191, Policy on the Acquisition and Utilization of Automatic Information Processing Resources (AIPR) and Data Processing Position**, update in progress) to meet their unit's legitimate needs in a timely fashion and in sufficient quantities to satisfy those needs.
8. All present employees and all new employees of DHMH with access to or potential access to computers shall sign the **State of Maryland, Code of Ethics**. The original signed copy shall be placed in the employee's personnel file maintained by his/her personnel officer, and a copy shall be placed in the work folder of the personal computer used by the employee.

**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

9. Employees of DHMH shall not make unauthorized copies of software products or software documentation.
10. Employees of DHMH shall not use unauthorized copies of software or software documentation.
11. Employees of DHMH shall not use their computers for any purpose other than official business.
12. Employees of DHMH shall abide by the Copyright Act of 1976, as amended from time to time, any license agreements that come with the computer software, and any other laws or regulations that are promulgated that relate to the copying of software products.
13. Where doubt exists as to whether copying is authorized or unauthorized, employees should contact the Director, Information Resources Management Administration, DHMH, or designee.

**D. AUTHORITY**

1. The Director, Information Resources Management Administration, DHMH, shall:
  - a. Irrespective of licensing provisions, define which software is authorized and permissible for use by DHMH employees on State owned computer equipment.
  - b. Establish and maintain centralized records of all software purchased by or through the DHMH headquarters.
  - c. Appoint a Software Manager who shall oversee implementation of and adherence to software policy established within DHMH.
  - d. On or before May 15 of each year, inform the Deputy Secretaries, Directors of Administrations, Superintendents of facilities or equivalent, Local Health Officers, Heads of independent units, and the Software Monitors that the acknowledgment for compliance with State policy and this policy for prevention of software copyright infringement is due in the Office of the Secretary, DHMH, by June 15 of the respective year and the procedure to follow.

**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

e. On or before June 1 of each year, inform the Secretary, DHMH and the Executive Assistant to the Secretary:

1) that the certificate attesting to DHMH's compliance with State policy on prevention of software copyright infringement should be signed by the Secretary of Health and Mental Hygiene no later than July 1 of the respective year and forwarded to the Secretary, Department of Budget and Management.

2) of the procedure by which they are to receive compliance acknowledgment from all units of DHMH.

2. The Director, Personnel Services Administration, at the request of and in coordination with the Director, Information Resources Management Administration, shall conduct classes for the purpose of training Software Monitors and employees. The classes will be conducted as part of the normal employee orientation program and when needed as ascertained by the Director, Information Resources Management Administration.

3. Deputy Secretaries or equivalent, Directors of Administrations, Superintendents of Facilities or equivalent, Local Health Officers, and Heads of Independent units shall:

a. Appoint a person or persons with a working knowledge of computers and with the authority to take the necessary action to prevent copyright violations to be a Software Monitor(s) for his or her respective unit or units.

b. Send, when appointed and whenever requested, the name of the appointed Software Monitor(s) to the Director, Information Resources Management Administration.

c. Report, through appropriate channels, to the Secretary, Department of Health and Mental Hygiene, by June 15 of each year, that their respective unit(s) comply with State policy and this policy for prevention of software copyright infringement (See Appendix II).



**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

4. Deputy Secretaries, in addition to duties enumerated in Section III. D. 3. shall:
  - a. Ensure that all units under their authority comply with State policy and this policy for the prevention of software copyright infringement.
  - b. Ensure that all units under their authority submit certificates of compliance, (See Appendix II), in a timely manner, through the appropriate channels.
5. Superintendents of Facilities or equivalent, in addition to duties enumerated in Section III. D. 3. shall:
  - a. Appoint one Software Monitor to be the Chief Software Monitor.
  - b. Inform the Director, Information Resources Management Administration, of the name of the person selected to be Chief Software Monitor.
6. Local Health Officers, in addition to the duties enumerated in Section III. D. 3. shall:
  - a. Establish and maintain centralized records of all software acquired by all units under their jurisdiction.
  - b. Ensure that all units under their authority comply with State policy and this policy for the prevention of software copyright infringement.
  - c. Submit compliance acknowledgment, in a timely manner, through the Director, Community and Public Health Administration.
  - d. Appoint one Software Monitor to be Chief Software Monitor.
  - e. Inform the Director, Information Resources Management Administration, of the name of the person selected to be Chief Software Monitor.

**DHMH POLICY 02.01.02**

**Cross-Reference: Information Resource Management Administration**

7. The Software Manager shall:
  - a. Conduct training for the designated Software Monitors, identifying specific duties and responsibilities.
  - b. Conduct training for the Chief Software Monitors of the facilities and local health departments with emphasis on the presenting of the DHMH Software Policy to new employees during employee orientation at their respective units.
  - c. Maintain communication with and provide assistance to all Software Monitors regarding the DHMH Policy, procurement, record maintenance, receipt and installation, virus protection, and manufacturers' licensing.
  - d. Present DHMH Software Policy to new DHMH Headquarters employees during employee orientation.
  - e. Conduct random computer audits on DHMH Headquarters computers to ensure compliance.
  - f. Report all incidents of computer software copyright infringement to the Director, Information Resources Management Administration, or designee.
  - g. Perform other related duties as requested by the Director, Information Resources Management Administration, or designee.
  
8. Software Monitors shall:
  - a. Periodically inform all of the employees for whom the Software Monitor is responsible, of this policy and the pertinent laws and heavy fines to which copyright violators are subject.
  - b. Ensure that the Code of Ethics is signed by each user or potential user of a PC and that the original is maintained by the Personnel Officer and a copy is maintained in the individual's work folder).
  - c. Identify the Primary User for each PC for which the Software Monitor is responsible.

**Cross-Reference: Information Resource Management Administration**

- d. Establish a work folder for each Personal Computer (PC) for which the Software Monitor is responsible.
- e. Identify each folder with:
  - 1) the name of the PC's primary user.
  - 2) the System Unit Description and Serial Number.
- f. Place in each work folder:
  - 1) Software Log (See Appendix III) containing, at a minimum, the information needed to comply with the Software Publishers Association (SPA) requirements and recommendations.
  - 2) Software License.
  - 3) Registration Form (copy).
  - 4) Signed Code of Ethics statement by the user or users of the PC (copy).
  - 5) Original System Diskettes which may be stored in another area if readily accessible.
  - 6) Print-out of the Self Audit.
- g. Register software with the respective manufacturer.
- h. Store original diskettes in a readily accessible centralized location or store in the work folder established for each PC.
- i. Maintain all other necessary records in a safe but readily accessible centralized location.
- j. Periodically conduct computer audits on all computers for which the Software Monitor is responsible.
- k. Implement virus protection measures.



## IV. REFERENCES

Copyright Act of 1976

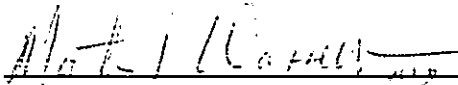
Software License Agreements

DBFP Manual #95-1, Prevention of Software Copyright Infringement,  
Department of Budget and Fiscal Planning, effective Date: June 1, 1995.

DHMH Policy 9191, Policy on the Acquisition and Utilization of Automatic Information Processing Resources (AIPR) and Data Processing Positions, effective April 2, 1987, (in process of being updated).

DHMH Memorandum, Subject: Computer Games, promulgated and signed by Martin P. Wasserman, M.D., J.D., Secretary, Department of Health and Mental Hygiene, dated May 30, 1995.

Approved:

  
Martin P. Wasserman, M.D., J.D.  
Secretary

Effective Date: May 12, 1998

Attachments:

Appendix I-

DBFP Manual 95-1, Prevention of Software Copyright Infringement

<b>MARYLAND STATE DEPARTMENT OF BUDGET AND FISCAL PLANNING MANUAL</b>	Number: 95-1    Effective Date: <u>June 1, 1995</u>
	Section: Office of the Secretary
	Subject: Prevention of Software Copyright Infringement

I. PURPOSE

To establish a uniform policy and procedure for prevention of software copyright infringement.

II. SCOPE

This policy applies to all officers and units of the Executive Branch of State Government.

III. DEFINITIONS

In this policy, the following words have the meaning indicated.

"Agency" means a unit of the Executive Branch of State Government.

"Authorized Software" means software used in accordance with the Software license or owned by the agency

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

"Software" means computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.

IV. POLICY

- A. The State will not permit the making or using of unauthorized software copies under any circumstances.
- B. 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.
- C. 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.
- D. The agency heads are responsible for ensuring that the agency is abiding by the terms of all software licenses.

Date 6/1/95

Page 1 of 4

IV. POLICY (cont'd)

- E. For additional authority and guidance in prevention of software copyright infringement and protection from computer viruses refer to the current version of the State Data Security Committee's STATE POLICY: DATA PROCESSING RESOURCES SECURITY and the Annotated Code of Maryland, Article 27, Section 146.

V. AGENCY RESPONSIBILITIES

- A. The agency head, or designee, is responsible for compliance with Federal copyright statutes and State software policy, maintaining adequate software records, and supervising compliance with this policy.
- B. The agency head shall implement the State of Maryland Software Code Of Ethics (see 95-1 Attachment 1). The Software Code Of Ethics (SCOE) shall be signed by all present employees and new employees at the time of hire for all employees with access or potential access to computers.
- C. The agency head, or designee, shall establish and maintain positive control of software, including inventory measures and accounting procedures that document all purchases of software. Each agency shall establish written procedures that include, as a minimum, the following.
1. Establishes control of all software and software licenses.
  2. Establishes a program that informs employees about the need to comply with software licenses.
  3. Maintains records of all software and software licenses.
- D. The agency head shall certify in writing each July 1st to the Secretary of Budget and Fiscal Planning that the agency is in compliance with this policy (see 95-1 Attachment 3).
- E. The agency head, or designee, shall establish a software compliance employee information program that:
1. Explains the SCOE and agency software policies.
  2. Informs employees about software piracy and why it is a problem. All new employees shall receive this information as part of an employee orientation program.
  3. Provides employees access to licenses for software used by the agency.

VI. ATTACHMENT

- A. Attachment 1 contains the format for establishing an agency Software Code of Ethics.
- B. Attachment 2 contains the format for agency head certification.

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:

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.

My signature indicates that I have read and understand this State of Maryland Software Code of Ethics. I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making or using unauthorized software may also subject me to civil and criminal penalties.

SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_

NAME: (Please Print): \_\_\_\_\_

AGENCY: \_\_\_\_\_

DIVISION: \_\_\_\_\_

LOCATION: \_\_\_\_\_

Date 6/1/95

Page 3 of 4



STATE OF MARYLAND

COMPLIANCE WITH STATE POLICY ON PREVENTION OF SOFTWARE COPYRIGHT INFRINGEMENT

DIRECTIONS:

\* This certificate shall be executed each July 1st and forwarded to the Secretary of Budget and Fiscal Planning. Compliance problems should be referred to the Department's Office of Information Technology for resolution.

THIS IS TO CERTIFY THAT \_\_\_\_\_  
(Agency Title)

COMPLIES WITH STATE POLICY FOR PREVENTION OF SOFTWARE COPYRIGHT INFRINGEMENT,  
DEPARTMENT OF BUDGET AND FISCAL PLANNING MANUAL ITEM NUMBER 95-1.

\_\_\_\_\_  
Agency Head Signature

\_\_\_\_\_  
Date

\* Date for initial certification extended until January 1, 1996.

Date 6/1/95

Page 4 of 4

**POLICY TO ASSURE CONFIDENTIALITY, INTEGRITY,  
AND AVAILABILITY OF DHMH INFORMATION****SHORT TITLE: INFORMATION ASSURANCE POLICY - IAP****I. EXECUTIVE SUMMARY**

This policy provides direction for certain actions of Department employees to assure confidentiality, integrity, and availability of DHMH information assets. It clarifies the roles and responsibilities of employees to protect the interest of DHMH and consumers regarding the release of non-protected information and safeguarding of DHMH protected and proprietary information. It recognizes and defines a life cycle for information. It acknowledges existing security and confidentiality requirements and initiates new requirements. It specifies requirements for both general and specific levels of due diligence and due care to be exercised over DHMH information. Additionally, it provides for protection levels that are commensurate with an acceptable level of risk of loss or disclosure.

Based on a "need-to-know" approach, supervisors are to assign employees an appropriate access authority and grant to them corresponding system access levels. Employees are held accountable for reading and complying with the corresponding section(s) of this policy and to act accordingly based on their assigned duties and responsibilities.

Due to the size, complexity, and evolving nature of health policy, information systems, and communications technology, this document provides broad standards for the handling and security of DHMH information. To facilitate compliance with this policy a separate document entitled "Security Procedures for DHMH Information Assurance Policies and Programs," hereafter referred to as "DHMH Information Security Procedures", has been developed to provide: (1) the roles and responsibilities of specific personnel, (2) data classifications, and (3) directions for handling Department information. These procedures are issued and maintained by the DHMH Information Resources Management Administration to support this policy.

**II. BACKGROUND**

State Government records are public records, under the Maryland Public Information Act (PIA) (see <http://www.oag.state.md.us/Forms/book.pdf>). Upon request, these records are to be made available for inspection or copying unless a provision of the PIA or other law either prohibits or authorizes the custodian to refrain from such a disclosure. However, certain health and medical information may be exempt from disclosure in order to protect the privacy of individuals. Therefore, DHMH must balance its responsibility, together with its other federal and State responsibilities, to protect the privacy and confidentiality of health and medical information and transactions.

Our communications with the public needs to reinforce a sense of trust in DHMH and State government. The Department's employees may be required to work with both electronic and paper-based systems, which included handling information, data, records, and documentation, hereafter generally referred to as information. Regardless of how information is obtained, created, or used in job performance, it must be handled with appropriate security precautions as established by this policy, or more restrictive applicable federal or State policies, procedures, regulations, or laws.

This policy seeks to both clarify the responsibilities of employees as well as to protect the interests of the Department and health consumers through the safeguarding of protected information. Any DHMH employees could be privy to information that is non-public, confidential, and/or intended only for Departmental use. Employees are cautioned that even seemingly appropriate disclosures of consumers' health and medical information may constitute an unwarranted 'invasion of privacy.'

The use of DHMH information systems by employees is explained in 02.01.01, Electronic Information Systems Policy ([http://indhmh/top\\_poly/policies/p020101.htm](http://indhmh/top_poly/policies/p020101.htm)). All DHMH employees are to sign and initial the appropriate section(s) of the Combined Policy Acknowledgement Form. To ensure employees' understanding and compliance with applicable provisions of this policy, the acknowledgment and signing of the form are to be done in consultation with supervisory staff who will also initial the form.

Because certain employees have duties that require them to have more extensive access, or require authority beyond that granted to the 'user' level, these employees are to read and comply with additional applicable provisions of this policy, as designated for *specific personnel* (see § III.A-Definitions) also consultation with supervisory staff.

As a condition of access to DHMH information resources, non-DHMH employees, or other individuals who access or use DHMH information systems, will also need to sign the Combined Policy Acknowledgment Form (see Appendix). Those individuals who do not sign the Statement will no longer be given access to or use of DHMH protected or proprietary information or information systems, which may result in subsequent job reassignment.

This policy was developed with assistance from the Security and Confidentiality (SeCon) Workgroup of the DHMH Health Information Coordinating Council which reviewed and applied federal and State statutes and regulations including the Health Insurance Portability and Accountability Act (HIPAA), in addition to the "best practices" of government agencies and private industry. Given the complexity and evolving nature of information systems and communications technology, this policy is to be reviewed and revised periodically in coordination with the DHMH Health Information Coordinating Council.

### **III. POLICY STATEMENTS**

#### **A. DEFINITIONS**

A comprehensive set of definitions for this policy is contained in *DHMH Information Security Procedures*, which may be access on the DHMH Intranet homepage at <http://indhmh/secpolicy/html/infosys.htm>.

**Specific personnel** - For the purpose of this policy, the term specific personnel refers to the following positions, which are also described and defined in detail in the DHMH Information Security Procedures.

- DHMH Institutional Review Board Official Custodian
- Custodian of Records
- Data Steward
- Designated Responsible Party
- Network (System) Administrator
- Database Administrator
- Data Technician
- Contract Monitor
- Contract Preparer

#### **B. INFORMATION SECURITY DIRECTIVES**

**1. Information Is to Be Protected.** All information, in any format, which is created or used in support of DHMH business, is to be considered either owned by DHMH or in DHMH custody. This information is a valuable asset and must be protected from its point of origin through its life cycle of creation, collection, maintenance, authorized sharing, and storage, until its lawful disposal. It is to be maintained in accordance with federal and State regulations and DHMH policies in a secure and reliable manner. Such protection levels are to reasonably assure confidentiality, integrity, accuracy, and ready availability for authorized use.

**2. Information Custodians Are To Be Appointed.** Program Directors, facility CEO's, Health Officers, and other executive managers of DHMH units are responsible for the information in their custody. Unless such responsibility is to be retained by them personally, or is provided for otherwise in law or regulation, the executives are authorized to appoint an official Custodian, Data Steward, or Designated Responsible Party to manage their information. These functions are also defined in the *DHMH Information Security Procedures*.

**3. Information Is To Be Classified.** Based on legal requirements, sensitivity, retention criteria, and the type of access required by authorized users, all DHMH information will be classified by its custodians, or other authorized authority.

**4. Protection Levels Are To Be Based on Risk Assessment.** *Information assurance* is to be achieved by implementing a comprehensive set of policies and procedures that protect against accidental or malicious disclosure, modification, or destruction. The level of effort to protect information should reflect its confidentiality and its risk of loss or compromise. The risk and impact of loss and the relative value of the information is to be determined initially, and annually thereafter, by the Director of the appointed custodian of the information set, using an IRMA-accepted business impact analysis tool as found in the *DHMH Information Security Procedures*. Additionally, a comprehensive risk analysis is required to be completed in the development phase of new information systems, or when existing systems are modified between annual reviews.

**5. Information Access Is To Be Granted On A "Need to Know" Basis.** Access to

information will be limited to authorized users who have a business need to know such information. This access and use will be further limited to appropriate job levels within legitimate job classifications. A higher level of access may be provided to persons who are designated to act in specialized support roles and who demonstrate a need to access, modify, or erase the information or to maintain the information system.

**6. A Separation of Duties is Required.** No single individual will have complete control of a business process or transaction from inception to completion. Custodians are directed to assure that there is functional segregation of roles and duties performed by an employee, to limit error and the opportunity for unauthorized actions.

**7. Employees and Contractors Are To Be Trained in Information Security Awareness and Ethics.** Depending on job duties, all DHMH employees and contractors and agents will be provided with training in information ethics. This training will be provided prior to access to DHMH information systems, or prior to commencement of contractual services, and annually thereafter.

**8. Employees Are to Be Aware of Their Obligation to Protect Information.** Laws and regulations specifically require maintaining the confidentiality of certain records. DHMH employees are responsible for knowing, or determining, in consultation with their supervisor, the specific protective requirements for information in their care, and for understanding their obligations to protect these resources. Employees are to report any suspected or realized violations.

### **C. ROLES AND RESPONSIBILITIES**

Every employee has a role and responsibilities to fulfill in *information assurance*. Employees' roles and responsibilities are described in more detail in the *DHMH Information Security Procedures*. They are necessary to direct, implement, enforce, and access the effectiveness of security and privacy

policy, planning, and administration. The success of this policy is dependent upon supportive management, appropriate role assignment, and employees' understanding of their roles and responsibilities for implementing and enforcing the policy. Every DHMH employee is assigned at least one role and its related responsibilities:

**1. Chief Information Officer (CIO)** - For the purpose of this policy, the DHMH CIO is responsible for providing guidance on all Information Technology issues. The CIO is also responsible for directing the management and administration of the DHMH information security program and initiating measures to assure and demonstrate compliance with security and privacy requirements.

**2. Information Assurance Officer (IAO)** - The IAO is directly responsible for the Department-wide coordination of all aspects of security and confidentiality, pursuant to applicable federal and State laws, regulations, and policies, and DHMH policies, procedures, and protocols. The following are the responsibilities of the IAO:

- develops and reviews system security and privacy policies and grants exceptions to them;
- provides guidance to assure the integrity of all DHMH information;
- reviews the security and confidentiality of the resources associated with the processing functions;

- reports security status of DHMH, as required;
- assures software controls are implemented;
- ensures procurement requirements of the IAP are met;
- supervises the resolving of security and privacy incidents;
- acts as Chief Privacy Officer (unless the role is otherwise assigned);
- coordinates with network security staff;
- assists in the preparation and review of IT risk assessments and contingency plans; and
- coordinates with internal and external audit staff to assure IAP requirements are included in audit reviews.

**3. Security Officer (SO)** - The DHMH SO serves as the single point of contact and as the access control agent for the daily IT security program. The following are responsibilities of the SO's:

- performs system audits, as directed;
- coordinates with DHMH Monitors for access controls;
- resolves authentication and authorization issues or concerns;

participates in addressing general security issues;  
provides appropriate IT security awareness and training to all employees;  
assists in the development of DHMH systems contingency and disaster recovery plans;  
functions as the daily operational central point of contact for any type of IT security related incidents or violations;  
disseminates information concerning security alerts and potential threats to all DHMH system owners;  
notifies users of security-related policies and procedures;  
assists in preparing annual systems evaluations of major processes including incident handling and security awareness training; and,  
assists in risk management analysis to determine effectiveness in reducing security incidents.

**4. Security Monitors (SMs)** - The DHMH System Monitors serve as the central point of contact and as the authorization control agents in their designated units for the daily IT security program. The following are SM responsibilities:

coordinates with the DHMH Security Officer in the preparation of lists of authorized users;  
makes changes to lists, and audits, as required;  
participates in addressing unit and DHMH security issues;  
participates in IT security awareness and training;  
performs as the central point of contact for unit-level IT security related incidents or violations;  
disseminates information concerning security alerts and potential threats to DHMH system owners;  
ensures that users are aware of security-related policies and procedures; and,  
assists in the annual systems evaluation process.

**5. User** - The User is an employee or agent or contractor who has access to DHMH information. Users are responsible for consulting with supervisory staff to:

determine the user's role and responsibilities to protect information resources in the user's control or possession  
understand and comply with all applicable DHMH and other security and privacy requirements, and  
to facilitate a better understanding of the general and specific requirements for the confidentiality of protected and/or proprietary information.

**6. Specific Personnel** - The positions previously listed under Section III A - Definitions - Specific Personnel, within the scope of their assigned duties, are instructed to implement the following provisions as necessary to protect information from inadvertent or intentional improper use or disclosure.

a. Information is to be Protected. Protection of information requires a diligent coordination of organizational and administrative requirements, physical security safeguards, and technological security measures further detailed in *DHMH Information Security Procedures*. <http://indhmh/secpolcy/html/iaphic2.htm>.

b. Employees Are to Actively Comply with IAP Requirements.

*Specific Personnel* are to act as required or directed in order to assure compliance with Federal, State and DHMH directives. They are to report any known or suspected violations of these directives, throughout the lifecycle of the DHMH information resources in their custody.

c. Proprietary Interests In DHMH Information Are To Be Maintained. *Specific personnel* are to assure the Department's proprietary interest in information is protected through both legal and administrative means, describing and documenting the qualities and limitations of DHMH information in their custody.

d. Information Must Be Collected, Maintained, Transferred, Stored, and Disposed of As Authorized. In accordance with applicable laws and regulations, employees who have access to information must be diligent to protect consumer rights and DHMH interests. *Specific personnel* may not transmit information electronically unless permitted by approved written procedures.

e. Employees Are Authorized To Release Non-protected Information to the Public.

*Specific personnel* will classify information in their custody, authorize certain employees,

establish procedures to prevent unintended disclosure, facilitate and clarify the decision-making processes related to release/sharing in accordance with DHMH copyright requirements.

f. Employees Will Not Allow the Unauthorized Sharing of Protected and Proprietary Information. The sharing of DHMH protected or proprietary information is encouraged as a good business practice, however, such sharing must be as necessary, appropriate and legal, in accordance with an explicit written understanding. DHMH protected or proprietary information will not be physically or electronically removed or shared, without the explicit authorization of the official custodian of record or designee.

g. Specific Personnel Will Not Allow the Unauthorized Disclosure of Protected and Proprietary Information. DHMH protected or proprietary information may only be disclosed to others if necessary, appropriate, legal, and only as authorized by the official custodian of record or designee.

h. Certain Specific Personnel Will Monitor the Sharing of Protected Proprietary Information - When information is shared or accessed, *Specific personnel* will establish and follow written procedures to hold all subsequently approved users to the same Department and/or other requirements and responsibilities. This includes an extension of the requirements and the continued strict adherence to all rules required by a DHMH recognized Institutional Review Board including resubmission requirements.

i. Certain Employees May Authorize Disclosure of Protected and Proprietary Information. Authorized *Specific personnel*, as defined in this policy, are permitted to disclose protected or proprietary information resources in the course of their official duties, only if the requirements of this policy or other more stringent requirements are met before such disclosure.

j. Employees Are To Notify Vendors Of The IAP And Other Applicable Requirements. - *Specific personnel* involved in the preparation and monitoring of DHMH contracts and memoranda of understanding (MOU) will ensure that vendors, agents, or other entities who provide work-for-hire, understand and comply with all applicable requirements for the protection of DHMH information resources. This will be required when such resources are shared, or when DHMH information systems are maintained, changed or developed.

k. Specific Personnel are Responsible for IAP Compliance. Persons designated or authorized to act in the capacity of *Specific personnel*, as defined above, are responsible for taking any and all reasonable, appropriate, and legal steps to ensure all employees comply with the terms of this policy.

#### **D. DISCIPLINARY, CIVIL AND CRIMINAL CONSEQUENCES**

Violation of this policy may result in disciplinary action up to and including separation from State service and civil or criminal penalties. These remedies include, but are not limited to, those specified in the Annotated Code of Maryland, SG §10-626 through §10-628, HG §4-309, and Crimes and Punishments Article 27 §45A.

#### **IV. REFERENCES**

Executive Order 01.01.1983.18- State Data Security Committee, State Agency Information Security Practices. <http://209.15.49.5/01/01.01.1983.18.htm>

Annotated Code of Maryland, Article 27, Sections 45A and 146, Prevention of Software Copyright Infringement.

Manual #95-1, Maryland Department of Budget and Fiscal Planning, June 1, 1995.

DHMH Policy 02.01.01, Policy On The Use Of DHMH Electronic Information Systems, effective June 5, 1998. [http://indhmh/top\\_poly/policies/p020101.htm](http://indhmh/top_poly/policies/p020101.htm).

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, effective May 12, 1998. [http://indhmh/top\\_poly/policies/p020102.htm](http://indhmh/top_poly/policies/p020102.htm).

"Security Procedures for DHMH Information Assurance Policies and Programs," DHMH CIO, IRMA, 2000. <http://indhmh/secpolcy/html/iaphic2.htm>.

#### **V. Appendices, Exhibits, & Addenda**

Combined Policy Acknowledgement Form  
Software Code of Ethics

APPROVED:

/s/ (signed copy on file) DATE: June 1, 2001

**Georges C. Benjamin, M.D., Secretary**

# 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><b>02.01.01 Policy on the Use of DHMH Electronic Information Systems (EIS)</b>                      I hereby acknowledge awareness of <b>DHMH Policy 02.01.01</b>, and that my use of these systems constitutes my consent to comply with this directive.</p>
		<p><b>02.01.02-Software Copyright Policy &amp; the State of Maryland Software Code Of Ethics-</b>                      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"> <li>1. <b>The State will not permit the making or using of unauthorized software copies under any circumstances.</b></li> <li>2. <b>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.</b></li> <li>3. <b>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.</b></li> </ol> <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. <b>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.</b></p>
.....	.....	<p><b>02.01.06-Policy to Assure Confidentiality, Integrity and Availability of DHMH Information (IAP)</b>                      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><b>02.01.06-IAP- "Specific Personnel" Acknowledgement</b>                      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 <b>specific personnel</b>.</p> <p>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 <b>specific personnel</b> 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.