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.

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 <u>and</u> 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 **<u>not</u>** 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 <u>job related</u> 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 <u>limited, minor, incidenta</u>l 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 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

APPROVED:

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

October 16, 2013
Effective Date