Department of Health and Mental Hygiene

Information Technology

Technical Security Policy,

Standards & Requirements

Version 4.0

Version Comment: Mandatory revision to

Meet state policy: version 3.0, 9/2011 & COMAR 10-1301-1308, Chapter 304

Approval Date: June 28, 2014

Mr. Kevin Naumann, CIO,
Department of Health and Mental Hygiene
Office of Information Technology

Distribution: DHMH Business units & Partners
Initiated By: Office of Information Technology (OIT)

Approval

_____ _____ Date

Kevin Naumann, Interim CIO

Recommended for approval

_____ _____ Date

Gerral Spence, CISSP, QA Manager

_____ _____ Date

David Bickel, Director, OIT Security Division

Table of Contents

PART I - Policy

Part 2 - STANDARDS & REQUIREMENTS (SAR)

The sections below correspond to their respective citations in the policy.

SAR-1 - DHMH IT Security Program (Revised 3-2013)

SAR-2- Software Code of Ethics (Revised 3-2013)

SAR-3- Policy Deviation Request (Revised 3-2013)

SAR-4- Combined Acknowledgment Form DHMH #4518 (Revised 3-2013)

SAR-5- System Inventory, Security Classification & Protection (Revised 3-2013)

SAR-6 - Dial-up- remote access (Revised 3-2013)

SAR-7 - Incident Response (Revised 3-2013)

SAR-8 - Data Eradication (Revised 3-2013)

SAR-9 – Laptop & Mobile Computing (Revised 5-11)

SAR-10 - Encryption (Revised 3-2013)

SAR-11- Wireless Networks (Revised 3-2013)

SAR-12 - Passwords (Revised 3-2013)

SAR- 13 - Firewalls (Revised 3-2013)

SAR-14 - Appropriate Use of Internet/ Social Media (Revised 3-2013)

SAR-15 - Attachment- Incident Response Protocol (Revised 3-2013)

SAR-16 - Attachment 2 - DHMH INFORMATION TECHNOLOGY SECURITY PROGRAM – Table

Additional reference material: State Government Article §§ 10-611 through 10-630, “Maryland Public Information Act”

Part I

PURPOSE & INTRODUCTION

The purpose of this policy is to describe and direct security requirements that DHMH and all agency information system owners must meet in order to protect the confidentiality, integrity and availability of state owned information.

This document provides a detailed, operations level policy with standards and requirements for information technology security. It applies to all business units in the Department of Health and Mental Hygiene. It establishes general requirements and responsibilities for protecting technology systems, in accordance with the Maryland State Information Technology Security Policy and Standards promulgated by the Department of Information Technology (DoIT).

The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, hardware, software, and many other more specialized resources.

The State's delivery of critical public services depends on availability, reliability and integrity of its information technology systems. *To better meet the needs of the agency, this policy and its standards and requirements exceed the State minimum requirements as set forth by DoIT.*

Our agency-wide security program is managed by the DHMH Office of Information Technology (OIT). This policy establishes a minimum standard and a consistent approach for security. See: SAR-1,"DHMH IT Security Program."

Some business units will also need to adopt stronger requirements due to the sensitive and/or confidential nature of their data. DHMH business units must participate with OIT in a process to review their special risks, and adopt appropriate methods to protect their information technology resources.

The common security approach also supports compatible security solutions shared among administrations, yielding a better return on technology investment.

Because of the rapidly changing information technology security environment the policy will be formally reviewed annually, and may require more frequent updates to remain current. Updates will be documented in the Record of Changes section below.

This policy is based on the statewide Information Technology Security Policy, Version 3.0, September 2011, issued by the Secretary of the Department of Information Technology (DoIT) under authority granted by the Annotated Code of Maryland Article § 3A-303 through 3A-305, and is the highly detailed iteration of DHMH Policy 02.01.01, "Employee Information Technology Security: Protecting Non-Public Information," February 2013, issued by the Secretary, DHMH.

Persons with questions or needing further information are encouraged to contact the OIT Information Security Program Manager, the Director, OIT Security Division, at (410-767-5219).

SCOPE

This policy covers all information that is electronically generated, received, transmitted, stored, printed, filmed, and typed as well as all associated equipment and contracted services. This policy and the accompanying Standards and Requirements (SAR), Part 2 of this policy, all hereinafter referred to as the "Policy" applies to:

- All DHMH business units and all of their IT systems, regardless of who is operating them, and their data assets,
- All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights. See: SAR-2, "Software Code."

OBJECTIVES

This policy defines the minimum standards and requirements to which each DHMH business unit, including employees and contractors, must adhere. The primary objectives of the IT Security Policy are:

- To establish a secure environment for the processing of data
- To reduce information security risk
- To communicate the responsibilities for the protection of information

PREVIOUS POLICY SUPERSEDED

This policy supersedes the directives mandated in the "State Agency Data Systems Security Practices" as revised (1999), and the original DHMH 02.01.01 (EIS), and is issued as the highly detailed iteration of the current DHMH Policy 02.01.01, "Employee Information Technology Security: Protecting Non-Public Information," February 2013, issued by the Secretary, DHMH.

AUTHORITY

The State DoIT has authority to set and subrogate to the agency the authority and responsibility for the development and implementation of policy and to provide guidance and oversight for security of all IT systems in accordance with the Annotated Code of Maryland as cited above. The DHMH CIO and designees has the singular authority and responsibility for the operation of network services and data communications infrastructure across the agency. This includes core services and related equipment and circuits provided within the agency data center, and at facilities and local health departments.

RECORD OF REVISIONS

Date	Revision Description
3/19/2013	Initial document executed
9/23/2013	Updated Table of Contents; corrected links.
10/1/2013	Updated language: removed GroupWise references, changed password rules to reflect "personal passwords" not to be revealed. (Bickel)

7/2014	Updated all data loss citations to reflect Personal Information (PI) and Protected Health Information (PHI); cited COMAR 10-1301-1308 for reporting of PII breaches.

SECTION 1: Preface

Information and information technology systems are essential assets of the State of Maryland. 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.

Each business unit within DHMH is responsible for compliance with this policy. Business units within DHMH are to use this policy as a minimum standard and guide when procuring information technology and communication services, service providers, contractors, software, hardware and network components to protect the confidentiality, integrity and availability of IT assets. Units unable to comply with these requirements must notify the DHMH Inspector General, Office of Corporate Compliance, and the CIO in writing. See: SAR-3,"Policy Deviation Request."

This security policy was developed in alignment and close parallel construction with the State policy. It includes Standards and Requirements (SAR) at a procedural level to ensure compliance with the policy. At the direction of the State CIO, DHMH has adopted NIST information security related standards and guidelines. In the event that a published NIST standard is deemed insufficient or non-existent, DHMH will adopt industry type-accepted security guidelines (or develop them) and refer to them within this security policy.

SECTION 2: Roles and Responsibilities

This policy sets the minimum level of responsibility for the following individuals and/or groups: Department of Information Technology; Agency (DHMH) & Business Units; and Employees and Contractors:

2.1 Agency Level (DHMH- Office of Information Technology- OIT)

Information security is an agency responsibility under the direction and leadership of OIT and shared by DHMH business units. DHMH Executive, Governance bodies, and unit management shall provide clear direction and visible support for security initiatives. OIT in coordination with the DHMH OIG, Office of Corporate Compliance, is also responsible for:

- Implementing and maintaining the Agency IT Security Program;
- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy;
- Monitoring and coordinating with the DHMH OIG, Office of Corporate Compliance, enforcement of the IT Security Program within the agency;
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency security program;
- Managing the Agency Security Program and initiating measures to assure and demonstrate compliance with security requirements;
- Ensuring that security is part of the information planning and procurement process;
- Implementing a risk management process for the life cycle of each critical IT System;

- Implementing an IT Security Certification and Accreditation process for the life cycle of each agency critical IT System;
- Identifying security vulnerabilities within Agency systems and recommending corrective action;
- Assessing the adequacy and coordinating the implementation of specific information security controls for new systems or services;
- Management of data communications infrastructure and related devices (hardware & software) and circuits across the agency to workstation and server levels;
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions;
- Assuming the lead role in resolving Agency information security and incidents;
- Documenting and ensuring that a process is implemented for the classification of information in accordance with the Policy for Classifying Confidential Information;
- Specifying the level of security required to protect all information assets under their control to comply with this Policy;
- Ensuring a configuration/change management process is used to maintain the security of the IT system;
- Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems in accordance with state IT Disaster Recovery Plan Guidelines;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users; and
- Ensuring that all DHMH business units are in compliance with this policy.

DHMH business units must work with OIT to identify critical systems and their 'data owners' (usually business unit managers) who are to be held responsible for:

- Assuring the continued security and integrity of the OIT-managed data communications infrastructure as described above;
- Conducting system security reviews and preparing/supporting mitigation plans;
- Classifying data & systems;
- Approving access and permissions to the data;
- Ensuring methods are in place to prevent and monitor inappropriate access to confidential data; and
- Determining when to retire or purge the data.

2.2 Employees and Contractors

All employees and contract personnel are responsible for:

- Complying with this policy See: SAR-4, "Combined Acknowledgement Form, DHMH #4518."
- Being aware and acknowledging their responsibilities to protect IT assets of their agency and the State
- Exercising due diligence in carrying out the IT Security Policy
- Being accountable for their actions relating to their use of all IT Systems
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State

SECTION 3: Asset Management

All major information systems assets shall be accounted for and have a named owner. Owners shall be identified for all major assets and the responsibility for the maintenance of appropriate controls shall be assigned. Responsibility for implementing controls may be delegated. Accountability shall remain with the named owner of the asset.

3.1 Inventory, Classification, and Assessment of IT and Data Assets

DHMH Business Units shall participate in the system listing, assessment, classification and protection/mitigation plans of their assets. Based on this information, levels of protection shall be implemented commensurate with the value and importance of their assets. Business Units will provide inventories of the important assets associated with each information system as part of the system security and disaster recovery plan. Each asset should be clearly identified and its ownership and security classification agreed and documented, together with its current location (important when attempting to recover from loss or damage) as follows:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster recovery plans, archived information;
- Software assets: application software, system software, development tools and utilities;
- Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units), furniture, accommodation;
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning. See: SAR-5, "System Inventory, Security Classification & Protection."

3.2 Information Security Classification Policy

This policy provides specific guidance and a process for data classification.

This policy pertains to all information within State of Maryland systems that is processed, stored, or transmitted via any means. This includes: electronic information, information on paper, and information shared orally or visually. Data and record custodians must adhere to this policy and educate users that may have access to confidential information for which they are responsible.

All Maryland State information is categorized into two main classifications with regard to disclosure:

- Public
- Confidential (non-public)

Public information is information that has been declared publicly available by a Maryland State official with the explicit authority to do so, and can freely be given to anyone without concern for potential impact to the State of Maryland, its employees or citizens. (See appendix item: "State Government Article §§ 10-611 through 10-630, Maryland Public Information Act" for authoritative detail on "Public Information."

Confidential describes all other information. It is understood that some information has the potential for greater negative impact if disclosed than other information, and hence requiring greater protection. Maryland State personnel are encouraged to use common sense judgment in applying this policy. If an employee is uncertain of the classification of a particular piece of information, the employee should contact their manager for clarification.

Confidential information must be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. Confidential information is prohibited on portable devices and non-state owned devices unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on any portable or remote access device must be encrypted. Exceptions to this may include contracted managed (outsourced) services where security of confidential information is documented, reviewed and approved by data custodians (or delegated authority). Approved storage on any portable device must be protected with FIPS 140-2 certified encryption technology. The penalty for deliberate or inadvertent disclosure of confidential information can range from administrative actions to adverse personnel actions up to termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

DHMH has further established and promulgated a policy that directs the protection of non-public information from disclosure to unauthorized individuals or entities, including other State or Federal agencies. The process shall be compliant with the Maryland Public Information Act and any applicable federal laws. Reference: DHMH 02.01.06 Information Assurance Policy – IAP on the DHMH Intranet under Information Technology.

All confidential information on paper or removable media MUST be clearly marked "Confidential" and will be subject to the following handling guidelines.

3.2.1 Guidelines for Marking and Handling State Owned Information

Information in the custody of the State which is classified by the originating authority (custodian/owner) shall be classified and protected at an equal level, or not accepted by State without caveats for custody and use.

- Public Information: Information that has no restrictions on disclosure.
    - Marking: No marking requirements.
    - Access: Unrestricted.
    - Distribution within Maryland State systems No restrictions.
    - Distribution outside of Maryland State systems: No restrictions.
    - Storage: Standard operating procedures based on the highest security category of the information recorded on the media. (*Refer to the System Security Categorization requirement in the following Section 3.3*).
    - Disposal/Destruction: Refer to Physical Security section of this document.
    - Penalty for deliberate or inadvertent disclosure: Not applicable.

- Confidential Information: Non-public information that if disclosed could result in a high negative impact to the State of Maryland, its' employees or citizens and may include information or records deemed as Private, Privileged or Sensitive.
    - Marking: Confidential information is to be clearly marked as "Confidential".
    - Access: Only those Maryland State employees with explicit need-to-know and other individuals for whom an authorized Maryland State official has determined there is a mission-essential need-to-share, and the individual has signed a non-disclosure agreement.
    - Not removed from State property without advanced, written authorization by a manager who has direct responsibility for the data.

- Distribution within State of Maryland systems; Delivered direct - signature required, envelopes stamped Confidential, or an approved, encrypted electronic email or electronic file transmission method.
- Distribution outside of State of Maryland systems: Delivered direct; signature required; approved private carriers; or approved encrypted electronic email or electronic file transmission method.
- Storage: Physically control access to and securely store information system media, both paper and digital, based on the highest security category of the information recorded on the media. Storage of Non-public information is prohibited on portable devices unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on any portable device must be protected with encryption technology using FIPS 140-2 validated cryptographic modules with approved modes of operation. Additionally, keep from view by unauthorized individuals; protect against viewing while in use and when unattended, store in locked desks, cabinets, or offices within a physically secured building.
- Disposal/Destruction: Dispose of paper information in specially marked disposal bins on Maryland State premises or shred; electronic media is sanitized or destroyed using an approved method. *Refer to Section 6.7, "Physical Security" section of this document.*

3.3 System Security Categorization Policy

DHMH Business units must use the OIT-provided Data Systems Inventory & Classification application to classify and document IT systems under their control in accordance with established System Sensitivity Designation Criteria. When the IT System is shared between State entities and/or between State, Federal, or local entities the highest level of classification will determine the classification of the data or IT System. For example, one agency may categorize the data at a medium level while the second agency may classify the data at a basic level, therefore, the data at both agencies will be at a medium level.

All parties sharing the IT System or data must agree to the initial classification and any change in the classification. An IT System shall clearly identify data that is considered non-public or public and any electronic exchange of data will clearly state that the information is non-public or public. See: SAR-5, "System Inventory, Security Classification & Protection."

SECTION 4: Security Control Requirements Overview

All agency information systems used for receiving, processing, storing and transmitting confidential information must be protected in accordance with these requirements. Agency information systems include the equipment, facilities, and people that handle or process confidential information.

This computer security framework was primarily developed using applicable guidelines specified in National Institute of Standards & Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* and (SP) 800-53 revision 3, *Recommended Security Controls for Federal Information Systems* and also Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*. Applicable NIST SP 800-53 controls designed to protect systems with a '**moderate**' category level, as defined in Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, are included in this policy as a

baseline. Systems with a 'high' category level should consult with the Director, OIT Security Division for guidance in applying appropriate additional security controls.

SECTION 5: Management Level Controls

5.1 Risk Management

A risk management process must be implemented to assess the acceptable risk to agency IT Systems as part of a risk-based approach used to determine adequate security for the system. Business units shall cooperate with OIT Security to analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Each unit will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system.

> See: Appendix SAR-5, "System Inventory, Security Classification & Protection."
>
> For additional guidance, refer to DHMH Information Assurance Policy (IAP) 02.01.06 and the NIST Special Publication 800-30, Risk Management Guide for Information Technology at http://csrc.nist.gov/publications/nistpubs ; See also: NIST Special Publication 800-39.

5.2 Security Assessment and Authorization

Agency Business Units shall participate in IT System risk assessment and security plan development. Completion and acceptance by the CIO of this plan and any mitigation processes in writing will stand as the system accreditation documenting that security controls have been adequately implemented to protect confidential information for each application system under their control. This written accreditation and acceptance by the agency CIO constitutes the Unit's completion of the security controls and completion of risk mitigation and evaluation as noted in Section 5. Custodians of confidential information must also sign this document to verify the completeness and propriety of the security controls used to protect it before initiating operations. This shall be done for any infrastructure associated with confidential information. A system review shall occur annually, and recertification shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security authorization.

Agency Business Units respectively shall continuously (at least annually) reassess the security controls within their information systems to ensure that the controls are operating as intended. OIT and Units shall authorize and document all connections from information systems to other information systems outside of the accreditation boundary through the use of service interface agreements and monitor/control system connections on an ongoing basis. Units shall periodically conduct a formal assessment of the security controls of information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for their systems.

Units are responsible to develop and periodically update a Plan of Action & Milestones (POAM) that shall identify any deficiencies related to the processing of confidential information. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during

internal inspections. A Corrective Action Plan (CAP) will identify activities planned or completed to correct deficiencies identified during the safeguard review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known vulnerabilities in agency systems - IRS Safeguard Guidance
http://www.irs.gov/businesses/small/article/0,,id=213693,00.html

5.3 Planning

Agency and Business Unit security planning controls include system security plans, system security plan updates and rules of behavior. Under OIT guidance and using an automated assessment tool, Business Units must develop, document, and establish a system security plan by describing the security requirements, current controls and planned controls, for protecting agency information systems and confidential information. The system security plan must be updated to account for significant changes in the security requirements, current controls and planned controls for protecting agency information systems and confidential information. Each system security plan must be maintained in SharePoint or in a similar secure environment and contain a set of rules describing their responsibilities and expected behavior for information system use for users of the information system.

NIST Guidance
http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Guide for Developing Security Plans for Federal Information Systems

5.4 Network Services - Internal/External Connections & Service Interface Agreements

Network services including hardware, software and communications infrastructure is the sole responsibility of OIT. All network devices are secured and managed by OIT, regardless of physical location or custody, and must remain under OIT control.

To comply with Privacy requirements only OIT network security staff is permitted to monitor network traffic and devices at any segment on the data network. Tampering with network devices or software, using unauthorized IP addresses, or monitoring network traffic outside these agency security requirements constitute a security breach and is a serious violation of this policy.

External network connections shall be permitted by OIT only after all approvals consistent with this Policy and other laws or regulations are obtained, and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by DHMH and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system IT Security Certification and Accreditation package and in the IT System security plan. An SIA shall include:

- Purpose and duration of the connection as stated in the agreement, lease, or contract
- Points-of-contact and cognizant officials for both the State and non-State organizations
- Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations
- Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection
- Requirements for notifying OIT-IND immediately of a suspected or actual security incident on the network
- A provision permitting the State to periodically test the ability to penetrate the State's network from the external network connection or system. See: SAR-6, "Dial-up & Remote Access ."

SECTION 6: Operational Level Controls

6.1 Awareness and Training

Business Units must ensure all information system users and managers are knowledgeable of security awareness material and sign the "Combined Policy Acknowledgement Form" before authorizing access to systems. Units must identify personnel with information system security roles and responsibilities, document those roles and responsibilities, and provide access to sufficient security training - before authorizing access to information systems or confidential information, and routinely thereafter.

Units must document and monitor as part of their overall HR management plan individual user's information system security training activities including basic security awareness training and specific information system security training.

All existing employees who have, or may have in the future, access to the DHMH LAN/WAN and/or non-public proprietary information must complete this training within six months of the issuance of this policy. This training is available via the DHMH Intranet "EmployeeCentral" under Information Technology, IT Security Training links. DHMH Employee Security Training

6.2 Configuration Management

System hardening procedures shall be created and maintained to ensure up-to-date security best practices are deployed at all levels of IT systems (operating systems, applications, databases and network devices). All default system administrator passwords must be changed. Agencies shall implement an appropriate change management process to ensure changes to systems are controlled by;

- Developing, documenting, and maintaining current secured baseline configurations.
- Developing, documenting, and maintaining a current inventory of the components of information systems and relevant ownership information.
- Configuring information systems to provide only essential capabilities.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and providing the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.
- Maintaining backup copies of hardened system configurations.

Security Configuration Guidance: National Security Agency;
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
Center for Internet Security;
http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks

6.3 Contingency Planning

As an adjunct to and in support of the agency COOP planning, Business Units under the guidance of OIT shall develop, implement, and annually test and validate to OIT an IT Disaster Recovery plan for all systems determined by the CIO or Unit managers to be Business Critical. A system is Business Critical if it supports the administration of an agency Critical Business Process as defined in the agency COOP plan.

Detailed disaster recovery guidelines can be found at:
http://doit.maryland.gov/support/Pages/SecurityDisasterRecovery.aspx

6.4 Incident Response

Information Technology Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. A computer incident within Maryland state government is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices.

DHMH has adopted a State-mandated common set of terms and relationships between those terms. The taxonomy below does not replace discipline (technical, operational, intelligence) that needs to occur to defend state agency computers/networks, but provides a common platform for data collection and analysis. DHMH Business Units shall utilize the following incident and event categories and report within an appropriate timeframe.

Category	Type	Description	Response Time
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a state agency network, system, application, data, or other resource	Immediate report by telephone and email to OIT and DoIT
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Immediate report by telephone and email to OIT and DoIT
CAT 3	Malicious Code	*Successful* installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Within 4 hours of discovery by OIT to DoIT by email
CAT 4	Improper Usage	A person violates acceptable computing use policies as defined in Section 10 of this document.	Within 7 business days by OIT to DoIT

Agency Incident Categories

Business Units shall report IT incidents to OIT by phone contact to the OIT Help Desk 410-767-6534 and completing an IT Incident Report linked below . For more details see: SAR-7,"Incident Response."

State-wide Government Intranet form access;
http://doit.net.md.gov/security/pages/sa.aspx
Downloadable form;
http://doit.maryland.gov/support/ASMsecurityForms/ITIncidentReportFmPrint.pdf

6.5 Maintenance

OIT or our vendors identify, approve, control, and routinely monitor the use of information system maintenance tools and remotely executed maintenance and diagnostic activities. Only authorized personnel are to perform monitoring or maintenance on network infrastructure or information systems.

OIT requires that Business Units conducting IT-related tests seek OIT approval and schedule tests to ensure that systems are not disrupted. Maintenance performed on or changes to base-line state of IT communication, data, or application systems shall be documented in accordance with manufacturer or vendor specifications in system administration logbooks and subject to review by OIT management and State and federal auditors.

6.6 Media Protection and Management

No IT equipment shall be released from a Business Unit's control until the data storage devices have been removed and rendered inoperative by the Business Unit, or removable media has been destroyed or conditioned so data are unrecoverable.

This policy applies to all electronic storage media equipment that is owned or leased by the State (including, but not limited to: workstations, servers, specialized lab diagnostic equipment containing any form of embedded memory, laptops, cell phones and communication devices, Multi-Function Printers/Copiers, and environmental or process control equipment). See: SAR-8, "Data Eradication," and SAR-2,"Software Code..."

All media that contains confidential information, as defined in this policy, including 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) shall be clearly labeled "Confidential". Agencies shall restrict access to system media containing confidential information to authorized individuals.

IT Systems and electronic media shall be protected and marked in accordance with their data sensitivity. Users shall not store data on electronic media that cannot be adequately secured against unauthorized access. Data to be electronically transferred to a remote storage location must be transferred and maintained only by an approved secure, encrypted method. Offsite storage of critical system data is required, but subject to manager approval. Backup copies are not to be taken offsite by state personnel without explicit manager authorization. Bonded, contracted services should be used for offsite storage and retrieval. See also Section 3.2.1 this policy

When no longer required for mission or project completion, media (tapes, disks, hard drives, etc.) to be used by another person or program within the agency shall be overwritten with software and protected consistent with the data sensitivity of which the IT storage media were previously used. Specific procedures shall be documented in the IT System Security Plan for critical systems. See: SAR-8,"Data Eradication."

When no longer required by the business unit and intended for disposal outside the agency (e.g. Gov Deals, local surplus, or gifting) all business units will remove, render inoperative before leaving its custody, and assure the destruction of electronic storage media. In case-by-case basis where it is documented that the storage media contained only public data, Business Units may contact OIT for approval to sanitize the media in accordance with NIST SP 800-88 Guidelines for Media Sanitization. A review of all media will be required by network personnel to assure that non-public information is not present, nor is recoverable by keyboard methods. *Note: Disposal of electronic storage media must be in compliance with the agency and Business Unit's document retention policy and litigation hold procedures.*

Business Units must use a tracking method to ensure "Confidential" system media reaches its intended destination.

6.7 Physical and Personnel Security

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas. DHMH business units and associates will directly or indirectly:

- Secure IT areas with controls commensurate to the risks;
- Ensure secure storage of media;
- Obtain personnel security clearances where appropriate.

Physical access controls must be in place for the following:

- Data Centers;
- Areas containing servers and associated media;
- Networking cabinets and wiring closets and communication systems;
- Power and emergency backup equipment;
- Operations and control areas.

Access to data centers and secured areas must be requested by the employee's direct supervisor to DHMH Central Services or to the manager responsible for the secured area, and is restricted to employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization will be:

- Based on frequency of need for access;
- Approved by the manager responsible for the secured area and reviewed annually, or as job duties change.

Each Business Unit is responsible for:

- Ensuring that all portable storage media such as hard drives, flash media drives, diskettes, magnetic tapes, laptops, PDA devices, DVDs and CDs are physically secured; See: SAR-9,"Laptop Security."
- Ensuring proper employee/contractor identification process is in place and that all workforce and visitors are issued and prominently display State issued identification at all times;
- Ensuring proper environmental and physical controls are established and maintained to prevent system disruption, or accidental or unintentional loss of information residing on IT systems;
- Ensuring that all physical access controls are auditable to a unique individual level.

Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

6.8 System and Information Integrity

For each system or database owned or under their control Business Units shall implement or assure implementation of system and information integrity security controls at the application and database levels, including flaw remediation, information system monitoring, information input restrictions, and information output handling and retention.

OIT is responsible for the common IT infrastructure serving Business Units, and Business units are responsible for securing the application system level, and database level to assure controls are in place to protect against malicious code (viruses, worms, Trojan horses) by implementing protections (anti-virus, anti-malware) that, to the extent possible. This includes a capability for automatic updates, Intrusion detection/prevention tools and techniques employed to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

IT systems must restrict information system input to authorized personnel (or processes acting on behalf of such personnel) responsible for receiving, processing, storing, or transmitting confidential information.

System owners, Administrators and Database Administrators must identify, document, and correct information system flaws. Additionally, they must receive and review: information system security alerts/advisories for critical software that they use (operating system, database software, etc.), system/application & database logs on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

System owners, Administrators and Database Administrators shall manage and protect system output during the entire system lifecycle in accordance with applicable federal laws, Executive Orders, directives, data retention policies, regulations, standards, and operational requirements.

SECTION 7: Technical Level Controls

7.1 Access Control Requirements

DHMH Business Units must cooperate with OIT to:

- Manage user accounts, including activation, deactivation, changes and audits.
- Enforce assigned authorizations that control system access and the flow of information within the system and between interconnected systems.
- Ensure all users and entities use the OIT Active Directory (AD) as their single authoritative identity source (vault) and credential, and ensure;
    - servers and workstations are under the OIT Active Directory (AD) forest,
    - users and devices login (at minimum daily) to the OIT-AD service, and
    - request permission from OIT in writing, in advance to install "local logon" device credentials.
- Ensure that only authorized individuals (employees or agency contractors) have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of 'least possible privilege" and "need to know".
- Identify, document and approve specific user actions that can be performed without identification or authentication. An example of access without identification and authentication would be use of a public web site for which no authentication is required.
- Ensure that the systems enforce separation of duties through assigned access authorizations.
- Enforce at all levels, the most restrictive access and least capabilities required for specified tasks.
- Enforce a limit of (4) consecutive unsuccessful access attempts during a (15) minute time period by automatically locking that account for a minimum of (10) minutes.
- Display the following warning before granting system access;

> *"This is a State of Maryland Information System. Access to this system is restricted to authorized users and its use is limited to approved business purposes.*
>
> *By clicking below on the LOG IN link **you are agreeing to follow applicable federal, State and agency policies,** and expressly consent to the monitoring of all activities.*
>
> *Any unauthorized access or inappropriate use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon or communicated over this system are the property of State of Maryland and may be used by the State of Maryland for any lawful purpose. Required IT security policies are available at* http://indhmh/infosec/pdf/DHMH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf

- Ensure that unauthorized users are denied access by ensuring that user sessions time out or initiate a re-authentication process after (30) minutes of inactivity.
- Authorize, document, and monitor all remote access capabilities used on its systems. Remote access is defined as any access to an agency information system by a user communicating through an external network, for example: the Internet. Virtual Private Network (VPN) or equivalent technology should be used when remotely accessing information systems. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption for transmission of data and authentication information. See: SAR-10, "Encryption."
- OIT is solely responsible for approving all connections, both internal and external, to the DHMH network. This includes connections to the Internet, local government networks, inter/intra

DHMH site, other third parties remote access and dial-in connections. These shall be identified, documented, managed, reviewed and reported annually to CIO. See: SAR-6, "Dial-up & Remote Access."

- Follow agency OIT requirements or seek approval from OIT for more restrictive, formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (only if required and in best interest of State). The procedures shall address the authorizations allowed to receive, transmit, store, and/or process confidential information.
- Agencies will establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or accessing the information system from the external information systems; and process, store, and/or transmit agency-controlled information using the external information systems.
- Authorize, document, and monitor all wireless access to its information systems. Wireless security guidelines are documented in SAR-11, "Wireless Guidelines."
- Devices which are not the property of, or under the control of an Agency (including any portable devices) are prohibited from accessing information systems without prior written approval by the CIO or other delegated authority. If approved, restricted access rights are required to provide protections equivalent to the Agency's protection of its own systems.

7.2 Audit & Accountability Control Requirements

- Information systems must generate audit records for all security-relevant events, including all security and system administrator accesses. Security-relevant events must enable the detection of unauthorized access to confidential information. System and/or security administrator processes will include all authentication processes to access the system, for both operating system and application-level events.
- Audit logs must enable tracking activities taking place on the system. Application and system auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of critical/confidential information by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application.
- Logs should be written securely to an external repository and not reside on the application or database server.
- The information system shall be configured to alert appropriate agency officials in the event of an audit processing failure and take the additional actions (e.g., shut down information system, overwrite oldest audit records, and/or write to an alternate storage location).

  Logs must record:
  - Additions, changes or deletions to data produced by IT systems
  - Identification and authentication processes
  - Actions performed and identities of system operators, system managers, system engineers, technical support, and system administrators
  - Emergency actions performed by support personnel and highly privileged system and security resources
  - Date and time of event
  - Event location (terminal, port, location)
  - User id of person performing or associated with the action /event.

- Type of event
- Source of event trigger
- Asset or resource name and type of access
- Success or failure of event

- Procedures must be developed to routinely (daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution. Information systems shall provide the capability to automatically process audit records for events of interest based on selectable event criteria and also provide report generation capabilities.

  To support the audit of activities or otherwise as required, Business Units must ensure that audit information is archived for a minimum of 3 years or until the Office of Legislative Audits completes the audit of the entity to enable the recreation of computer related accesses to both the operating system and to the application wherever confidential information is stored.

  Information systems must protect audit information and audit tools from unauthorized access, modification, and deletion. Access to security logs must be limited to authorized audit or investigative personnel whose duties are sufficiently separated from operations.

7.3 Identification & Authorization & Access Control Requirements

DHMH Business units must ensure that information is accessed by the appropriate persons for authorized use only. Each unit must implement at a minimum the following:

- An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system
- An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and "need-to-know"
- An audit trail process to ensure accountability of system and security-related events

- Information systems must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics.
- System owners/operators must manage user accounts assigned within its information systems. Effective user account management practices include (i) obtaining authorization from appropriate officials (unit supervisor and data or system owner/custodian approval required) to issue user accounts to intended individuals; (ii) disabling user accounts, when no longer needed, in a timely manner; (iii) archiving inactive or terminated user accounts; and (iv) developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by information systems.
- Additionally the following are required:
  - user IDs are disabled after sixty (60) days of inactivity and notification to appropriate management to verify removal after ninety (90) days of inactivity
  - all default access capabilities are removed, disabled, or protected to prevent unauthorized use.
  - access privileges are traceable to a unique user id,

- provide an automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon, when technically feasible,
- user passwords shall be distributed from the password source in a way that only the intended recipient receives them,
- Self service password reset systems shall use a minimum of two challenge questions.
- Information systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
- Whenever information systems are employing cryptographic modules, the agency shall work to ensure these modules are compliant with NIST guidance, including FIPS PUB140-2 compliance.

7.3.1 User Authentication & Password Requirements

All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as "Functional ids". Functional ids are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., ACF id used to run production jobs). Passwords associated with functional ids are exempt from the password construction or sharing and change requirements specified below.

All DHMH employees, including contractors and vendors, are responsible for selecting and securing their passwords in accordance with the requirements in SAR-12,"Passwords."

7.4 System & Network Communications Control Requirements

DHMH Business Units shall assure the following for the design and operation of systems and services under their local control, and network services provided by OIT:

- Information systems shall separate front end interfaces from back end processing and data storage.
- Information systems shall prevent unauthorized and unintended information transfer via shared system resources.
- Information systems shall be configured to monitor and control communications at the external boundaries of the information systems and at key internal boundaries within the systems.
- Information systems must protect the confidentiality of non-public information while stored, and during electronic transmission. Additionally, non-public information must be encrypted on all media. When cryptography (encryption) is employed within information systems, the system must perform all cryptographic operations using Federal Information Processing Standard (FIPS) PUB140-2 validated cryptographic modules with approved modes of operation. When Public Key Infrastructure (PKI) is used, Agencies shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. See: SAR-10, "Encryption."

  Unless otherwise permitted by the CIO, the Director of OIT/IND is the single PKI and Certificate Authority holder of record and control agent.

- Whenever there is a network connection (external to the system), the information system shall terminate the network connection at the end of a session or after no more than (15) minutes of inactivity.
- Minimum Critical System requirements include implementing or allowing to be implemented by OIT:

    - Cryptographic solutions (encryption) when the confidentiality or sensitivity of information must be maintained while a message is in transit between computing devices and when confidential or sensitive information is stored in a file or database.
    - A routinely updated appropriate anti-virus, anti-spyware and file extension blocking solutions at the gateway entry points and on the desktop and server systems to prevent these systems from being compromised.
    - A firewall or other boundary protection mechanism is in place and has the ability to evaluate (1) source and destination network addresses, and (2) determine the validity of the service requested. See: SAR-13, "Firewalls."
    - Appropriate Intrusion Detection System and Intrusion Prevention System (IDS/IPS) solutions at the correct network location(s) and monitor to detect when the agency is under attack so an effective detection and defense strategy can be deployed.
    - An appropriate change management process to ensure changes to systems are controlled.
    - Separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
    - Procedures to implement an agreed upon backup policy and strategy , including the extent (e.g., full or differential/incremental), frequency, offsite storage, testing, physical and environmental protection, restoration, and encryption.
    - Security provisions for and segregation of certain internal data and systems from other data and systems on the networks.
    - Utilize only DHMH routable IP addressing scheme provided by OIT/IND for all networks, clients, systems, etc.
    - Connections to or maintenance of any network not routable via the DHMH core infrastructure is prohibited.
    - Restrictions on placing confidential or sensitive data on any application servers, database servers, or infrastructure components that require direct access from the Internet. Components that meet these criteria must be placed behind a de-militarized zone (DMZ) where they are not accessible from the Internet and can only interact with DMZ components through a firewall.
    - Appropriate procedures to protect documents, computer media, information/data, and system documentation from unauthorized disclosure, modification, removal, and destruction, including suitable measures to properly dispose of media when it is no longer needed.
    - Procedures and standards to protect information and physical media containing information in transit, including using facsimile machines, exchange agreements between the agency and external parties, transportation of physical media, and monitoring (e.g., audit logging, monitoring system use.)
    - Appropriate levels of security monitoring including intrusion detection, penetration testing, and violation analysis.
    - Documented reviews of audit trails on a regular basis to alert Business Unit custodians to inappropriate practices.

- Preventive or detection controls are in place to decrease or identify the threat of unintentional errors or unauthorized users accessing the system and modifying data.
- Appropriate data/document retention policies as dictated by the agency's policies, standards, legal and business rules.
- Appropriate documentation and adequate off-site electronic and backup storage of security policies and procedures, business contingency plans (COOP), disaster recovery plans, all related recovery materials and data, and incident response plans, including a plan for cyber attacks, such as a denial of service attack.

SECTION 8: Virtualization Technologies

Business Units must plan and test prior to the installation of virtualization solutions to ensure that the virtual environment is as secure as a non-virtualized environment and in compliance with SDLC and all relevant state and/or agency policies. See required guidance in sections 4 & 5 of NIST SP 800-125 *Guide to Security for Full Virtualization Technologies* shall be adopted as the state standard for securing virtualization solutions.

http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
NIST Guide to Security for Full Virtualization Technologies

SECTION 9: Cloud Computing Technologies

OIT requires assurances that security controls are in place for cloud-based applications that are commensurate with or surpass those used if the applications were deployed in-house. NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing.*
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
and, Cloud Computing Synopsis and Recommendations;
http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

SECTION 10: Electronic Communications Policy

The State encourages the use of electronic communications and electronic communications systems to enhance efficiency. Electronic communications and electronic communications systems are to be used 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.

For operational details see: SAR-14, "Appropriate Use…"

SECTION 11: Social Media

Social media is content created using highly accessible Internet-based publishing technologies used to share opinions, insights, experiences, and perspectives with others. These emerging collaboration platforms offer new ways for State employees to build citizen and agency relationships. Social media can also be used by State employees to take part in national and global conversations related to activities

within the State. The State of Maryland and DHMH has prepared guidance to be followed by all employees in the conduct of State business via these venues.

For operational details see: SAR-14, "Appropriate Use…"

SECTION 12: Policy Violations & Enforcement

Data leakage incidents such as disclosure of non-public information, or making inappropriate public statements about or for the State/Agency, or using State resources for personal uses, and harassing or inappropriate behavior toward another employee can be grounds for reprimand or dismissal.

In conference with DHMH Senior Management, the DHMH OIG and CIO will coordinate to recommend the appropriate corrective measures necessary to address the violation or finding of non-compliance. In accordance with State regulations and the law, disciplinary action, up through termination, may be warranted in cases of severe negligence or abuse.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of non-public information may result in civil and/or criminal penalties.

KEY DEFINITIONS

Term / Acronym	Definition
Acceptable Risk	A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accountability	A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.
Accreditation	The authorization and approval granted to operate a system or network in order to process sensitive data in an operational environment.
Agency	All units of the Executive branch excluding the University System of Maryland.
Approved Electronic File Transmission Methods	Includes approved: Virtual Private Network (VPN) tunnels supported by Executive Departments and Independent State Agencies; secure email, file encryption systems, some application-based password protection schemes e.g MS Word, Excel etc.
Authentication	The testing or reconciliation of evidence of a user's identity.
Authorization	The rights and permissions granted to an individual (or process), which enables access to a computer resource.
Authorized Software	Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.
Availability	Ensures the reliable and timely access to data or computing resources by the appropriate personnel.
Certification	A technical review made as part of and in support of the accreditation process.

	Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. A judgment and statement of opinion that the accrediting official can use to officially accredit the system is produced.
CIO	Chief Information Officer.
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical systems.
Computer	An electronic, magnetic, optical, 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.
Confidentiality	Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.
Confidential Information Non	Public information that is deemed private, privileged or sensitive. (See: DHMH Information Assurance Policy, (IAP)
Critical	Essential for continued operation.
Data Remanence	Residual information left behind once media has been in some way erased.
DHMH Business unit	An Office or Administration within the Department of Health and Mental Hygiene. For purposes of this policy, a Board, Commission, Facility or Local Health Department is considered an DHMH business unit if it is part of the DHMH wide area network.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet

Electronic Communication	Including, but not limited to, messages, transmissions, records, files, data, and software,
Electronic Communication Systems	Including, but not limited to, hardware, software, equipment, storage media, electronic mail, telephones, voice mail, mobile messaging, Internet access, and facsimile machines.
Encryption	The process of transforming information (referred to as plain text) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special
Incident	Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.
Identification	Data uniquely labeling a user to a system.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Information Custodian	The business function owner responsible for the information assets for a particular IT system.
Integrity	Freedom from corruption or unauthorized modification; internal and external consistency.
OIT	The Office of Information Technology within the Department of Health and Mental Hygiene.
OIT-IND	The Infrastructure/Network Division within OIT.
IT Systems	Automated systems: communications systems including wireless systems, computer

	hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.
ITEPP	Information Technology Emergency Preparedness Plan, including the business continuity plan, the recovery plan and the business resumption plan.
MCERT	Maryland's Computer Emergency Response Team. Team to be activated in the event of a major IT related disaster.
Media clearing	Media clearing is the removal of sensitive data from storage devices in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system functions. The data may still be recoverable, but not without unusual effort.
Mobile Code	Code that can be transmitted across the network and executed by a recipient.
Network	A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.
Network, Untrusted	Any network not controlled by the State agency.
NIST	National Institute of Standards and Technology.
Non-public	Non-public is information that is not subject to inspection and copying under the Maryland Public Information Act or federal law (e.g. Protected Health, Personally Identifiable, and reserved Proprietary Information)
Non-repudiation	Authentication with a high assurance to be genuine and that can not subsequently be refuted.
DoIT	The Department of Information Technology is the Executive State agency with oversight for state information resources under the direction of the State CIO.

Perimeter Access	Access to all entry and exit points of the network, controlled by firewalls and other filtering mechanisms.
Personal Use	Use of I.T. systems for purposes that are not job related.
PI	For the purpose of this policy- Personal Information as defined in COMAR 10-1301-1308, Chp.304
PHI	Protected Health Information as defined in federal statute: 45 CFR 160.103
Policy	For purposes of this document means the Executive Policy, and the directive Policy Standards and Requirements document.
Privacy	The level of confidentiality and protection that information is given in a system.
Privileged	Records protected from disclosure by the doctrine of executive privilege which may include but not limited to records: • Relating to budgetary and fiscal analyses, policy papers, and recommendations made by the Department or by any person working for the Department; • Provided by any other agency to the Department in the course of the Department's exercise of its responsibility to prepare and monitor the execution of the annual budget; • Relating to a State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity; • Of confidential advisory and deliberative communications relating to the preparation of management analysis projects conducted by the Department pursuant to State Finance and Procurement Article, §7-103, Annotated Code of Maryland. include but not limited to records:
Public	Public Information means information that may be inspected and copied under the

	Maryland Public Information Act. (See Appendix " State Government Article §§ 10-611 through 10-630, Maryland Public Information Act"
Requirements	For purposes of this document means policy, standards, and requirements.
Residual Risk	The portion of risk that remains after security measures have been applied.
Risk	The probability that a particular threat will exploit a particular vulnerability of an IT System.
SDLC	Systems Development Life Cycle as defined in the State of Maryland SDLC Methodology.
SIA	Service Interface Agreement.
Sensitive	Information that, if divulged, could compromise or endanger the citizens or assets of the State.
Social Media	Online technologies and practices that people use to share opinions insights, experiences, and perspectives with each other. e.g. Twitter, Facebook, etc.
Software	Computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.
Split Tunneling	Simultaneous direct access to a non-DHMH network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DHMH network via a VPN tunnel. The DHMH VPN Virtual Private Network (VPN) solution is the only approved method for remote access to the DHMH network via "tunneling" through the Internet.
Standard	Detailed implementation guidance established in policy by DoIT and prepared by OIT that governs the use of IT resources. Synonymous with Requirements.

VoIP	Voice over Internet Protocol, providing telephony services over IP networks.

PART 2 Standards & Requirements

The sections below correspond to their respective citations in the policy the contents of which are under the authority of the DHMH CIO.

SAR-1 - DHMH IT Security Program (Revised 3-2013)

SAR-2- Software Code of Ethics (Revised 3-2013)

SAR-3- Policy Deviation Request (Revised 3-2013)

SAR-4- Combined Acknowledgment Form DHMH #4518 (Revised 3-2013)

SAR-5- System Inventory, Security Classification & Protection (Revised 3-2013)

SAR-6 - Dial-up- remote access (Revised 3-2013)

SAR-7 - Incident Response (Revised 3-2013)

SAR-8 - Data Eradication (Revised 3-2013)

SAR-9 – Laptop & Mobile Computing (Revised 3-2013)

SAR-10 - Encryption (Revised 3-2013)

SAR-11- Wireless Networks (Revised 3-2013)

SAR-12 - Passwords (Revised 3-2013)

SAR-13 - Firewalls (Revised 3-2013)

SAR-14 - Appropriate Use of Internet/ Social Media (Revised 3-2013)

SAR-15 - Attachment- Incident Response Protocol (Revised 3-2013)

Additional reference material: State Government Article §§ 10-611 through 10-630, "Maryland Public Information Act"

Revised 3-2013

Title: SAR-1: DHMH Information Security Program

Policy Section: Roles and Responsibilities

Scope: These standards and requirements govern all users of any DHMH information or network resource. These standards apply to all data and information systems which reside on DHMH data processing systems (PCs, mid-range and mainframe), local area and wide area networks, as well as any computer data belonging to DHMH whether or not this data resides on the DHMH equipment or is connected to the DHMH network.

Requirements: It is a State requirement for all Executive agencies to establish and maintain an agency-wide Information Security program to assure the confidentiality, integrity, and availability of data and information on agency and agency-controlled information technology and communication systems.

The State-level I.T. security requirement issued by the Department of Information Technology, State CIO, (DoIT-CIO), applies to all Executive agencies of the State of Maryland, and establishes general standards, requirements, and responsibilities for protecting technology systems. Additionally, it directs each agency to internally develop and manage a IT Security Program that assures each agency Business Unit participates in the department-wide program, and further establish and implement appropriate unit-level portions of its own technology security plans

To meet the internal requirements, the DHMH CIO has assigned the implementation responsibility for the DHMH I.T. Security program to the Director, OIT Security Division, the Information Assurance Coordinator, an OIT employee. Responsibility for compliance with and enforcement of this policy is

vested by COMAR with the Office of Legislative Audit (OLA), and within DHMH with the Office of the Inspector General (OIG) as part of the Internal Audit/Corporate Compliance function.

The I.T. Security Program controls and concept of operations shall include but are not limited to the following:

1. **All information is covered:** Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services;
2. **Protection is based on risk, and in any situation:** Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed;
3. **Controls to be implemented**: Ensuring that risks to information security are identified and controls implemented to mitigate these risks;
4. **Administrative oversight required**: Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards;
5. **Training and Compliance required**: Ensuring that all employees and contractors understand and comply with the DHMH IT Security Policy, these standards and requirements, as well as all applicable laws and regulations;
6. **Physical Controls are directed**: Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's IT assets.

The DHMH Information Security Program is required to:

1. Implement an IT Security Certification and Accreditation process for the life cycle of each agency critical IT System;
2. Report to the DHMH CIO, as required on the status of the agency's IT Security Program
3. Enforce the state and DHMH IT Security Policies, Standards, and Requirements;
4. Manage the program and initiate measures to assure and demonstrate compliance with security requirements;
5. Assure DHMH Business Unit compliance with policy requirements to assure the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions;
6. Assume the lead role in resolving security and IT-related privacy incidents;
7. Document and ensure that a DHMH-wide process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard and Requirement;
8. Specify the level of security required to protect information assets under the control of DHMH Business Units to comply with the DHMH IT Security Policy;
9. Generate and monitor all IT Information Security Deviation/Risk Acceptance request in accordance with DHMH IT Security Policy, standards and requirements;
10. Maintain a listing of DHMH IT Systems that are certified by the CIO as being "Critical" in accordance with the DHMH IT Security Policy, Standards and Requirements definition.
11. Assure Business Units develop, implement and test IT Disaster Recovery Plans for each of their critical IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
12. Ensure a configuration/change management process is implemented and maintained for all Critical systems to assure the security of the IT system;

13. Assure Business Units which are permitted administer virus prevention, intrusion detection, and participate in an incident reporting program that coordinates with State efforts;
14. Ensure critical systems implement appropriate separation of duties and assign manager-authorized system permissions and responsibilities for agency system users.

The following are elements of the DHMH Information Security program in which Business Units must participate:

Each Business Unit in DHMH is responsible for participating in the implementation of the DHMH IT Security Program to secure the agency's communications, computer systems, networks, and data in accordance with DHMH and the State IT Security policies, standards, and requirements. The status of an agency IT Security Program will be reported to the State CIO on an annual basis. This standard specifies the major components that comprise the DHMH IT Security Program, and which must be included in and/or flowed by every corresponding DHMH Business Unit IT Security Program. Modifications or additions to this Standard and requirements will be issued by the OIT as required to respond to emerging IT security issues and changes in technology.

1. Management of the DHMH IT Security Policy, Standards, and Requirements;
2. Risk Management & Assessment;
3. System Certification and Accreditation
4. Systems Development Life Cycle Methodology;
5. Disaster Recovery Planning;
6. Security Awareness Training;
7. Communications and Operations Management
8. Access Control;
9. Information Security Critical Incident Response Process;
10. Compliance

Details on each component of the DHMH IT Security Program are in the Attachment 1 of this document, and in Attachment 2, Table format with roles and responsibilities – provided at the end of this document following SAR-15 for formatting reasons.

References: http://doit.maryland.gov (search for Security Program Requirements)

Attachments: Because we recognize the level of detail required to provide a comprehensive planning and implementation document, we have provided two level of documentation:

- **Attachment 1** is a highly detailed program document, and
- **Attachment 2** is a simplified table.

Attachment 1 is a program document in which each program element is described in detail so as to provide sufficient background detail and guidance to high-level management and

Executive staff, IT supervisory managers, program staff, and auditors, and acts as the high-level agency operational IT Security concept of operations document.

Attachment 2 is in table format and contains a brief description of each requirement with corresponding implementation directives. This format is provided to assist Business Unit staff and managers to understand the basic requirements, their role in each requirement, and to facilitate compliance with the provisions.

Attachment 1: DHMH Information Technology Security Program

The following details the scope of the DHMH Information Technology Security Program and is the basic concept of operations for the agency information and communications security program. Compliance with these requirements at the agency Business Unit level is the responsibility of the unit Director or top-level manager. Compliance monitoring is the responsibility of DHMH Office of the Inspector General (OIG) and the Maryland Office of Legislative Audits (OLA). Further information on these requirements can be accessed by contacting the Information Security Program Director in OIT at 410-767-6830.

Section 1: Policy management

Policy Management refers to the practices and methods used to create and maintain security policies to translate, clarify, and communicate management's position on high-level security principles. DHMH has adapted State policy, standards, and requirements to better reflect the corporate culture and needs of the agency.

Agency information security policies, standards, and requirements address the fundamentals of agency information security governance structure, including:
• Information security roles and responsibilities.
• Statement of security controls baseline and rules for exceeding the baseline.
• Rules of behavior that DHMH users are expected to follow and minimum repercussions for noncompliance.

To assist Business Units and contractors to achieve compliance with the policy, we have developed supporting guidance and procedures on how to effectively implement specific controls across the enterprise based largely on federal guidance e.g. NIST Special Publications and FIPS e.g. 800-66, "HIPAA Security…", and others as noted in the guidance.

OIT manages this policy, standards, and requirements to assure our directives are sufficiently current to accommodate the information security environment, the agency mission, and operational requirements. To ensure that information security does not become obsolete, OIT conducts an annual policy review and periodic revision cycle. As establish in DHMH Policy 02.01.03, part of the periodic review and ratification by the DHMH IT governance body. he discussions ensure that all internal security policies (i.e. IT, physical, personnel, communications, and operations) are sufficiently coordinated to ensure effective implementation of crosscutting and convergent security objectives.

http://csrc.nist.gov/groups/SMA/fisma/index.html

1. Federal Information Security Management Act (FISMA) Implementation Project
2. NIST 800-66, "HIPAA Security"
3. 800-39, "Managing Risk…
4. 800-61, Computer Incident Handling.."
5. DHMH Policy 02.01.03, "The Acquisition & Utilization Of Information Technology Resources."

Section 2: Risk Management

DHMH has established a process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This is largely a systems-based review when new systems are developed, or major, critical systems are modified substantially so as to warrant a reassessment.

The assessment process is used to assess the acceptable risk to DHMH IT systems as part of a risk-based approach used to determine adequate security for the system. Business Units developing systems are directed to include in the cost of the system development an initial pre-design consultation and a final security review and systems analysis process to be conducted by an external OIT-approved vendor.

Security assessments and reviews shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk.

DHMH and agency Business Units will cooperatively define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system. DHMH uses NIST Special Publication 800-30, Risk Management Guide for Information Technology for guidance: http://csrc.nist.gov/publications/nistpubs/ and our assessment standards and requirements as a basis for such analysis.

This process will typically encompass three processes: assessment, mitigation, and evaluation.

Section 3: System Certification and Accreditation

Security *accreditation* is the official management written decision given by DHMH CIO in cooperation with the Business Unit Director to authorize operation of an information system and to explicitly accept the risk to agency/Business Unit: operations, assets, or individuals based on the implementation of an agreed-upon set of security controls.

The DHMH CIO has the authority to oversee the budget and business operations of all DHMH information systems (DHMH Policy Number: 02.01.03, Policy On The Acquisition And Utilization Of Information Technology Resources http://www.dhmh.maryland.gov/SitePages/p020103r.aspx

The intention of Security accreditation is to provide a form of quality control and challenge managers and technical staff at all levels to implement the most reasonable and effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints.

By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

Based on system criticality and scope, OIT staff and Business Unit representatives will determine and document for the CIO approval a Certification and Accreditation plan.

Initial C&A may require a review and re-accreditation depending on significant changes in the system operating environment e.g. successful malicious attack, data loss, access control breach etc.

More detail can be found at:

http://doit.maryland.gov/support/Pages/SecurityCertAccreditation.aspx
Introduction to the State of Maryland IT Security Certification and Accreditation Guidelines;

Section 4: Systems Development Life Cycle

DHMH Business Units shall ensure that security is an integral part of the development and maintenance of their information systems, which include operating systems, infrastructure, applications and off-the-shelf products, services, and user-developed applications. Business Units shall work with OIT staff to identify and agree upon security requirements prior to the development and/or implementation of information systems and be documented as part of the overall business case. The requirements must also ensure compliance with any applicable laws, regulations, statutes, or state policies (e.g., HIPAA, PCI Standards, etc.). Security shall be considered and designed in from the beginning and during the entire system development lifecycle and funded as part of the system development and maintenance expenses of the sponsoring Business Unit.

DHMH Minimum Required Information Assurance Elements – other elements to be determined during the assessment and analysis phase:
• Implement requirements for ensuring authenticity and protecting message integrity in applications.

• Implement the use of encryption (cryptographic) measures to protect confidential or sensitive information and protect encryption keys from modification, loss and destruction at rest, and in transit.
• Implement input/output data validation checks to ensure data is correct and appropriate.
• Implement processes to control the installation of software on operating systems.
• Implement procedures to select, protect, and control test data. DHMH policy does not permit the use of live data in a production environment or use of primary production data sets in a test environment.
• Limit access to program source code and place source code in a secure environment, internally or 3rd party escrow for vendors.
• Implement change control procedures to minimize the corruption of information systems.
• Limit modifications to vendor-supplied software packages.
• When outsourcing software development, assure contractual language for licensing arrangements, code ownership, quality and security functionality, testing to detect malicious code, and escrow arrangements in the event of a declaration of third party failure that authorize DHMH to receive code or data upon demand without the intervention of the third party.

Important Resources
http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-55 Security Metrics Guide for Information Technology Systems
NIST SP 800-44 Guidelines for Securing Public Web Servers
NIST SP 800-66 HIPAA Security Implementation
State SDLC Planning Documents (DoIT.maryland.gov)

Section 5: Disaster Recovery Planning

Business Units shall develop, implement, and test an IT Disaster Recovery plan using OIT-approved materials a for each critical system to ensure that contingency procedures will be available in the event of a disaster resulting in the loss of services from the primary production system, which will successfully recover the system. Creation, maintenance, and annual testing of a plan is required with annual testing.

Important Resources
http://doit.maryland.gov/support/Pages/SecurityDisasterRecovery.aspx

Section 6: Security Awareness

OIT provides on-line and on-going face-to-face IT Security training to assure that users, unit managers, executive staff, and technical personnel understand their role and responsibility for information security. This program ensures employees and contractors know about information security and privacy relative to their job responsibilities. Business Units are required to participate annually in the IT security training as a condition of access to DHMH IT system resources.

Additionally, an OIT IT Security awareness program promotes the agency's existing policies, standards, and practices, and also targets various groups (such as employees and contractors, IT staff, or managers and supervisors) with information pertinent to their respective roles. This awareness program:

• Promotes security awareness using techniques such as: posters, email messages, formal instruction, web-based instruction, videos, newsletters, and security awareness days.
• Ensures all users annually sign confidential and acceptable use statements.
• Trains all users to quickly identify threats, and how to respond to security incidents.
• Informs all users about agency policies and procedures.
• Regularly reviews and updates training content to reflect changes to the agency's environment.

Important Resources:

1. DoiT Cyber security Training

2. DHMH Information Security Training for Managers, Network Specialists, System Administrators, and Users, 2013 rev. (PowerPoint and web-based) TRAINING LINK

Section 7: Communications and Operations Management (Information Assurance)

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it.

DHMH Business Units are required to assure that the key elements of system and communications protection are adequately applied to critical systems. They must include: backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code. Business Units are directed to assure that adequate processes to administer and monitor the technologies are provided commensurate with the system classification and the corresponding required level of security.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities. As always, it is a balance of these types of controls against business requirements, cost, efficiency, and effectiveness.

Operations management covers information technology assets throughout their lifecycle. Business Units are required to assure the implementation of proper operations management safeguards all of the organization's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers.

The appropriate level of protection that is applied will be based on (1) value and (2) criticality. (1) the information's value e.g. health- and personal-related information may have a high intrinsic value and potential financial or physical losses resulting from loss or compromise, (2) the ongoing business need for the information, particularly relevant when continuous availability (i.e., round-the-clock processing) is required.

DHMH Required Minimum Elements:
• Implement OIT-approved cryptographic solutions (encryption) when the confidentiality or sensitivity of information must be maintained while a message is in transit between computing devices and when confidential or sensitive information is stored in a file or database.
• Deploy and routinely update appropriate anti-virus, anti-spyware and file extension blocking solutions at the gateway entry points and on the desktop and server systems to prevent these systems from being compromised.
• Ensure a firewall or other boundary protection mechanism is in place and has the ability to evaluate (1) source and destination network addresses, and (2) determine the validity of the service requested. Only OIT/IND is authorized to install or permit the installation of and manage firewalls or other boundary protection mechanisms in DHMH.
• Deploy appropriate Intrusion Detection System and Intrusion Prevention System (IDS/IPS) solutions at the correct network location(s) and monitor to detect when the agency is under attack so an effective detection and defense strategy can be deployed.
• Implement an appropriate change management process to ensure changes to systems are controlled.
• Provide for separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
• Establish procedures to implement an agreed backup policy and strategy, including the extent (e.g., full or differential/incremental), frequency, offsite storage, testing, physical and environmental protection, restoration, and encryption.
• Secure certain internal data and systems (e.g. Personally identifiable & Protected Health Information, PII/PHI, Accounting, and Human Resources- social security numbers) from other data and systems on the networks.
• Separate protected information on application servers, database servers, or infrastructure components that require direct access from the Internet. Components that meet these criteria must be placed behind a de-militarized zone (DMZ) where they are not accessible from the Internet and can only interact with DMZ components through a firewall.

• Establish appropriate procedures to protect documents, computer media, information/data, and system documentation from unauthorized disclosure, modification, removal, and destruction, including suitable measures to properly dispose of media when it is no longer needed.
• Establish procedures and standards to protect information and physical media containing information in transit, including using facsimile machines, exchange agreements between the agency and external parties, transportation of physical media, and monitoring (e.g., audit logging, monitoring system use.)
• Implement appropriate levels of security monitoring including intrusion detection, penetration testing, and violation analysis.
• Perform timely reviews of audit trails and promptly alert security and management to inappropriate practices.
• Ensure preventive or detection controls are in place to decrease or identify the threat of unintentional errors or unauthorized users accessing the system and modifying data.
• Implement appropriate retention policies as dictated by the agency's policies, standards, legal and business rules.
• Implement appropriate documentation such as security policies and procedures, business contingency plans, disaster recovery plans, and incident response plans, including a plan for cyber attacks, such as a denial of service attack.

Important Resources:

DHMH IT Security Policy, 02.01.01, (User level policy) and this companion Technical Standards and Requirements document.

http://csrc.nist.gov/publications/PubsSPs.html

1. NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook
2. NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
3. NIST SP 800-45 Guidelines for Electronic Mail Security
4. NIST SP 800-83 Guide to Malware Incident Prevention and Handling
5. NIST SP 800-88 Media Sanitization Guide

Section 8: Access Control

Business Units are required to implement sufficient access controls (Identification, authorization, and authentication) to ensure that system resources are only available to users who are entitled to them. The objective is to prevent unauthorized disclosure of the agency's information assets. Key components include identification, authentication, and authorization. These components apply to people, process, and technology devices.

Identification is the process for establishing who someone or what something claims to be. The identity may be a person, a program, a computer or data.

Required authentication methods include passwords, fixed IP addresses, security tokens, smart cards, biometrics, and secret information known only to the person.

Required authorization describes the process of appropriate management granting privileges to users based on an authenticated identity and the users need for the least-privileged access required to conduct business.

Business Units are required to use authorization processes include signed and manager-approved access control forms for new employees, signed contracts between entities granting information rights, or assignment to a specific group or role. The access rights to the information shall be programmed or entered into the security system via an access list, directory entry, or view tables, for example, so the authorization rules are enforced.

DHMH Required Practices are to:
• Establish formal procedures for the owners, or owner designee, of the data to authorize access to information systems and services that use their data.
• Audit access level rights at regular intervals.
• Monitor and audit system access and use.

• Ensure the security system can identify and verify the identification and, if necessary, the location of each authorized user.
• Apply access method of “least privilege” where access to, or the flow of information, is only granted to the extent necessary to get the job done.
• Authenticate individuals and technology components consistent with acceptable risk levels determined by the information owners.
• Use state proscribed logon banners to display a general security notice and acceptance of use conditions.
• Promptly remove access upon employee termination or when the need no longer exists.
• Enforce the DHMH establish password standards (Section SAR:7 of this document) such as minimum length requirements with a combination of characters and numbers, and appropriate periodic password aging.
• When technically feasible, restrict connection time to appropriate business hours.
• Initiate automatic logout or password protected screen savers by the system after a specific period of inactivity.

Section 9: Information Security Critical Incident Management

Information Security Critical Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. A critical incident is an event or condition that can shut down business, disrupt operations, cause physical damage; or that can threaten the agency’s financial or public image. Examples of critical incidents could include activity such as:
• Unwanted disruption or denial of service
• The unauthorized use of a system for the processing or storage of data
• Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

All DHMH Business Units are required to follow the OIT-approved IT Incident response process provided as an attachment in SAR-15, “Incident Response.”

The term damage means “impairment to the integrity or availability of data, a program, a system or information”. DHMH OIT has the responsibility to report critical incidents to the DoIT Service Desk (410) 260-7778 or ServiceDesk@doIT.state.md.us Appendix A contains the Computer Security Critical Incident Handling Form.

Section 10: Compliance

The DHMH Chief Information Officer, CIO, DHMH, is responsible for compliance with this policy. The DHMH OIG, Office of Corporate Compliance is responsible for the enforcement of this policy. The DHMH CIO, or the agency’s delegated Information Technology professional, shall develop and implement the DHMH IT Security Program to implement this policy and these requirements and standards. Where the agency’s Business Units are unable to comply with this policy, immediate protection of information assets must be implemented and communicated to the OIG and CIO, and a timetable to resolve the discrepancies and controls for compliance shall be included. The controls shall include but are not limited to:

• Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services;
• Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed;
• Ensuring that risks to information security are identified and controls implemented to mitigate these risks;
• Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards;
• Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations
• Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State’s IT assets security program. Not only should the risk management program engage changes to

existing systems, but should also integrate into the agency's operational functions, as well as the System Development Life Cycle (SDLC) for new systems and applications.

Important Resources:
http://csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Standards & Requirements – SAR-2

Revised 3-2013

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: _____

STATE OF MARYLAND

COMPLIANCE WITH STATE POLICY OF PREVENTION OF SOFTWARE COPYRIGHT INFRINGEMENT

DIRECTIONS: This certificate shall be executed each July 1st and forwarded to the Secretary of Budget and Management. Compliance problems should be referred to the

DoIT Office of Information Technology for resolution.

1.3 THIS IS TO CERTIFY THAT _____

Agency

COMPLIES WITH STATE POLICY FOR PREVENTION OF SOFTWARE COPYRIGHT INFRINGEMENT,

DEPARTMENT OF BUDGET AND MANAGEMENT MANUAL ITEM NUMBER 95-1.

_____ _____

Agency Head Signature Date

PURPOSE

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

SCOPE

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

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, or communications facility that is directly related to or operated in conjunction with a device or system.

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

POLICY

The state will not permit the making or using of unauthorized software copies under any circumstances.

The State will provide legally acquired software to meet legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.

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.

The agency heads are responsible for ensuring that the agency is abiding by the terms of all software licenses.

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, Criminal Law, Section 7-302.**

AGENCY RESPONSIBILITIES

The agency head, or designee, is responsible for compliance with Federal copyright statues and State software policy, maintaining adequate software records, and supervising compliance with this policy.

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 by new employees at the time of hire for all employees with access or potential access to computers.

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:

Establishes control of all software and software licenses.

Establishes a program that informs employees about the need to comply with software licenses.

Maintains records of all software and software licenses.

The agency head shall certify in writing each July 1st to the Secretary of Budget and Management that the agency is in compliance with this policy (see 95-1 Attachment 3).

The agency head, or designee, shall establish a software compliance employee information program that:

Explains the SCOE and agency software policies.

Informs employees about software piracy and why it is a problem. All new employees should receive this information as part of an employee orientation program.

Provides employees access to licenses for software used by the agency.

ATTACHMENT

Attachment 1 contains the format for establishing an agency Software Code of Ethics.

Attachment 2 contains the format for agency head certification.

Title: Security Deviation Request/Risk Acceptance

Policy reference: SAR-3: Policy & Requirements - Deviations

Scope: All DHMH Administrations, Facilities, Local Health Departments, our State agency or private partners, contractors and their sub-contractors, and volunteers, are directed to follow this Requirement.

Requirements: If an organizational unit determines that it cannot comply with a provision of the DHMH IT Security Policy and Requirements, an Information Security Deviation Request/Risk Acceptance form (attached) must be submitted by the DHMH Administration Director to the DHMH CIO.

Procedures: Complete the attached form and submit to DHMH CIO.

Attachment: **"**IT Security Deviation/Risk Acceptance Form"

IT Security Deviation/Risk Acceptance Form

General requirements for seeking a security deviation

- Requests for deviations must be made in writing on this form to the CIO.
- Proposed deviations will be considered on an individual basis
- Complete this form. You may be requested to conduct a systems risk assessment using an OIT provided tool that identifies and helps your staff and your AAG to evaluate the threats, countermeasures and extenuating circumstances associated with the proposed deviation and its actual or potential impact on IT systems
- Administration Director sign and send to the DHMH CIO. All deviation requests require the concurrence of your AAG, the approval of the DHMH CIO, the Secretary, and the State CIO.
- Please provide an adequate lead time for review.
- Deviations, if granted, are for a maximum period of twelve (12) months after which time the deviation will be considered expired and require renewal.
- In accordance with SG 10-611 (j) of the Maryland Public Information Act the details of Security Deviations will be not be released without redaction by the CIO because exposing operational details could pose a security threat to state IT systems.

SECURITY DEVIATION REQUEST

Date of request: _____

The undersigned are requesting a security deviation as identified below.

Unit requesting Security Deviation_____

Explain what is non-compliant:

_____

_____

Why compliance cannot be met:

_____

_____

Explain what risks may result from non-compliance:

_____

_____

Proposed alternative and/or compliance plan

_____

_____

DHMH Director_____ Date_____

AAG _____ Date_____

Disposition: Approval/Disapproval

DHMH CIO _____ Date_____

Secretary _____ Date_____

State CIO _____ Date_____

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Title: SAR-4: Combined Acknowledgement Requirement & Form

Policy reference: Appropriate Use- User Agreement

Scope: These requirements govern all users of any DHMH network resource. These requirements apply to all network resources which reside on DHMH local area and wide area networks, as well as to any computer system, data, or information belonging to or in the custody of DHMH whether or not this data resides on the DHMH network.

Requirements: As a condition of access, all employees, contract personnel, and volunteers are responsible for:

- Being aware and acknowledging their responsibilities to protect IT assets of their agency and the State
- Exercising due diligence in carrying out the IT Security Policy
- Being accountable for their actions relating to their use of all IT Systems
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State
- Complying with this policy by signing the attachment to this SAR: "Combined Acknowledgement Form, DHMH #4518)

The DHMH employees, contractors and vendors must meet the criteria in this document prior to issuance of any information technology device, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

Organizational Unit sanctions for non-compliance with these requirements include disconnection from DHMH LAN/WAN until modifications are made that meet state and OIT security requirements.

Procedures: Complete the form and provide to your supervisor/manager.

Attachments: "Combined Acknowledgement Form #4518" Rev Nov 2001/ Jan 2010

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

SAR-4: COMBINED POLICY ACKNOWLEDGMENT FORM- DHMH #4518

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- Initials		**Policy Number-Statements**	
Employee	Supervisor	**02.01.01 DHMH Information Technology Security Policy** Policy, Standards and Requirements for the protection of Information Technology. 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.	
		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. **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.** 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**.	
		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. **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 ***specific personnel***. 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 ***specific personnel*** provisions of the IAP and guidance.	

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.

DHMH 4518 (REV Nov 2010) This form will be retained in the employee's DHMH personnel file.

Title: SAR-5: IT System Inventory, Security Classification & Protection

Policy reference: Section - Device & Media Controls

Scope: These standards govern all users of any DHMH information or network resource. These standards apply to all data and information systems which reside on DHMH data processing systems (PCs, mid-range and mainframe), local area and wide area networks, as well as any computer data belonging to DHMH whether or not this data resides on the DHMH equipment or connected to the DHMH network.

Requirements: An IT System shall clearly identify its data contents as Non-Public or Public, with the intention of ensuring that system owners/users are aware of the sensitivity of data to be handled and ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.

DHMH employees, contractors and vendors must meet the criteria in this document for any State issued information technology device or information resource, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

This requirement further codifies the policy and procedural directives of DHMH Information Assurance Policy – IAP (02.01.06) that provides direction for certain actions of Department employees to assure confidentiality, integrity, and availability of DHMH information assets. You are directed to consult the IAP for further policy-level data security details.

This requirement is based on NIST publication FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) and

> …establishes security categories for systems that process public and non-public information. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

This requirement further requires that system owners or custodians DHMH information systems are identified and that systems are classified as to the type of information they can be process, verify that they are authorized in regulation or law, be listed on an official Department Data Systems Directory, complete an OIT-approved risk assessment, and a security and operations plan, be accredited for such use by the DHMH CIO, and undergo frequent security and operational review by their owners and designated security personnel.

NOTE: the classification process does not certify a system as appropriate for processing a specified level of data. The completion of an approved System

Security Plan and a form of certification and approval for processing from the CIO determines if the system is appropriately conditioned and protected to operate at a stated classification.

The following requirements include:

A.) Data Processing Sensitivity Classification Required
B.) Legal Collection Authorization Required
C.) Listed on DHMH Systems Inventory
D.) System Security & Operation Plan Required
E.) CIO Certification & Accreditation Required
F.) Frequent Security Reviews Directed

IT systems processing protected or proprietary data (and in some cases public data where determined by the CIO) must complete an appropriately detailed level of a system development lifecycle and management plan that includes:

A) Classification as to the sensitivity level of data they contain using the attached document
B) Documentation of authorization for such use in law or regulation,
C) Listing the system on the official DHMH Data Systems Inventory,
D) Completion of an approved risk assessment, security, and operations plan,
E) Accreditation and certification for such use by the DHMH CIO or designated accrediting authority, see DoIT Certification & Accreditation Guidelines (based on NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems,) and
F) Participation in security and operations review.

Procedures: The following procedures are directed to meet the above Requirements.

A.) Data Processing Sensitivity Classification Required
B.) Legal Collection Authorization Required
C.) Listed on DHMH Systems Inventory
D.) System Security & Operation Plan Required
E.) CIO Certification & Accreditation Required
F.) Frequent Security Reviews Directed

A) Classify the system as High (contains NON-public information), MODERATE, or LOW (contains Public information).

Use the following processes and refer to the attached document for more detailed guidance to assist in the classification process.

1) Does the system contain NON-Public information?
If **NO**, complete items C and F.

If **YES**, classify the system as HIGH and complete the following items:

Use the FIPS-199 (attached) to classify and establish a processing level.

2) Describe and document the information handled by the system and identify the overall system security level as LOW, MODERATE, or HIGH.
   i) This element includes a general description of the information, the information sensitivity, and system criticality; which includes requirements for confidentiality, integrity and availability, auditability and accountability as directed under FIPS-199.

B) Document your organizations authorization for such use in law or regulation,
   1) Include all citations that authorize the system to collect and process information e.g. COMAR, Federal statute etc.

C) List the system in the DHMH Data Systems Inventory,
   1) Access the web-based inventory provided by OIT 410-767-6830 for more information.

D) Complete an approved risk assessment, security, and operations plan. See DHMH adaptation of NIST 800-26, "Security Self Assessment Guide for Information Technology Systems,"

E) Seek memo of accreditation and certification for such use by the DHMH CIO or designated accrediting authority, see DoIT Certification & Accreditation Guidelines (based on NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems,) and

F) Participate in annual or more frequent security and operations review.

Attachments:

(1) FIPS 199, *Standards for Security Categorization of Federal Information and Information*, February 2004

(2) DHMH adaptation of NIST 800-18/26, "Security Self Assessment Guide for Information Technology Systems." (available on the DHMH "Employeecentral" InfoSec site)

Attachment 1: Excerpt: FIPS 199, *Standards for Security Categorization of Federal Information and Information*, February 2004

(3) CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

This publication establishes security categories for both information[1] and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

[1] Information is categorized according to its *information type*. An information type is a specific category of information

(e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Security Objectives

The FISMA defines three security objectives for information and information systems:

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is **LOW** if—

− The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[2]

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—

− The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

[2] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

The *potential impact* is **HIGH** if—

− The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Security Categorization Applied to Information Types

The security category of an information type can be associated with both user information and system information[3] and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system (see description of security categories for information systems below). Establishing an appropriate security category of an information type essentially requires determining the *potential impact* for each security objective associated with the particular information type.

The generalized format for expressing the security category, SC, of an information type is:

> **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
>
> where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.[4]

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

> **SC** public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of

integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category, SC, of this information type is expressed as:

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

[3] System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

[4] The potential impact value of *not applicable* only applies to the security objective of confidentiality.

Security Categorization Applied to Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.[5]

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

EXAMPLE 4: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

[5] It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the

interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)}, and **SC** administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}, representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as: **SC** SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

Table 1 summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**

Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. (*public info)*	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. *(PII/PHI)*	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. *(location of response drug stockpile during a public health emergency)*
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES "

End of excerpt. Full FIPS-199 is available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Attachment (2): DHMH adaptation of NIST 800-18/26 & 33, "Security Self Assessment Guide for Information Technology Systems" (current version available on the //INDHMH InfoSec site)

Original issue date: March 19, 2013
Last review date: June 28, 2014
Review frequency: Annual
Review by: Information Technology Governance Board
Approved: Kevin Naumann, Interim CIO
Signature: _____

Revised 3-2013

Title: SAR-6: Dial-Up and Remote Access

Policy reference: Access & Authorization

Scope: These requirements govern all users, employees, contractors, vendors and agents with a State-owned or personally-owned computer permitted to connect to the DHMH/State network. This applies to all network resources which reside on DHMH local area and wide area networks, as well as to any computer system, data, or information belonging to or in the custody of DHMH whether or not this data resides on the DHMH network. This applies to remote access connections used to perform work on behalf of DHMH including reading or sending email and viewing intranet web resources.

Remote access implementations include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, WiFi, wireless broad-band, and cable modems.

Requirements: The DHMH Virtual Private Network (VPN) and access control tokens provided by OIT-IND is the only approved method of user remote access. The following services are prohibited except where they are specifically approved by the Agency CIO. Some may require a formal Deviation Request (attached)

- Any product or method that attempts to or bypasses the DHMH-provided solution.
- Dial-in desktop modems when operating in conjunction with a LAN connection.
- Use of any type of “remote control” product or service (i.e. PCAnywhere, GoToMyPC) when not used in conjunction with the DHMH VPN.
- Use of any monitoring tools e.g. environmental processes, SCADA etc.
- Storage of confidential information on any non-state owned device is prohibited. Confidential information may not be stored on any state or personally owned portable device without prior written approval from agency CIO (or delegated authority). Approved storage on any portable device must be encrypted using DHMH-approved encryption scheme.

It is the responsibility of DHMH employees and contractors with remote access privileges to the DHMH/State network to ensure that their remote access connection has the same level of security and privacy controls as the user's on-site connection at DHMH.

All remote access users are required to comply with DHMH IT security policies and the following:

1. Remote access must be strictly controlled by the use of unique user credentials which meet DHMH strong password design requirements, and preferably token-based access.

2. Remote access passwords are to be used only by the individual to whom they were assigned and may not to be shared.

3. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize an approved encryption scheme.

4. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted.

5. All hosts that are connected to DHMH internal networks via the approved DHMH VPN remote access technology must have up-to-date anti-virus software implemented and the latest current operating system security patches installed.

6. Personal equipment that is approved by the CIO for business use to connect to the DHMH networks must meet the standards and requirements of DHMH-owned equipment for remote access. Further, OIT does not provide technical support for personal equipment.

7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the DHMH network must obtain prior approval from CIO.

8. DHMH employees, contractors and vendors must meet the criteria in this document for any State issued information technology device, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

Organizational Unit sanctions for non-compliance with these requirements include disconnection from DHMH LAN/WAN until modifications are made that meet State and OIT security requirements.

Procedures: Employees who are authorized by their management to use remote access are to contact their local area network administrator and request a remote access solution using the DHMH Virtual Private Network and access control tokens.

In addition, the following controls for dial-in modems, when permitted, must be implemented:

1. Use unique network access user IDs different from their application or network user ID;
2. Set answer or pickup until after sixth 6th ring;
3. OR the use of a dial-up modem security device (see Dial-up Request attachment) in place of items 1 and 2,
4. Access privileges must be prohibited to any applications except those expressly required (i.e. cannot grant access to entire network, must be application specific);
5. Conduct an annual review of access requirements to determine if the dial-up/remote practice can be replaced with a less risky access method.

Detailed Procedures:

A.) Primary Protection Objective
B.) Remote Access - Dial-up Alternatives
C.) Required Modem settings
D.) Remote access details not public information and on a need-to-know basis.
E.) Risk Acceptance Agreements Required
F.) Periodic Verification
G.) Dial-up Permission Based on Questionnaire Reponses
H.) Exception Process

A) The primary protection objective is to assure there is no potential for a simultaneous connection between the DHMH WAN/LAN and a third party network (Internet or other non-network Maryland network).

B) Remote Access - Dial-up alternates are provided below in descending order of preference as examples, are not the exclusive methods of protection, and may not be acceptable in all cases:
   1) The use of a DHMH Virtual Private Network account (VPN) and a token access control device managed by OIT is the only approved remote access method in DHMH.
   2) Isolated PCs or servers on the DHMH WAN/LAN.- Acceptable isolation includes stand-alone machines, machines in an OIT-approved DMZ, or machines residing on LAN segments that have services limited so as to assure acceptable isolation from DHMH LAN/WAN resources.
   3) The use a single or combination of modem access control device(s) that provide adequate and reasonable protection, as determined during application for such use, from external probing and direct compromise attempts (e.g. refuses incoming calls, and controls incoming/outgoing dialing sessions. See http://www.cpscom.com

C) Set modem to out-calling only.
   1) Modems must be set not to answer calls. Since this usually means the setting is controlled by a script, additional precautions must be taken to assure no incoming calls are permitted if the modem is reset to default settings.
   2) Perform an initial test to verify that this setting is not defeated by the modem powering-off and recycling.
   3) Perform this security test at least annually to verify continued compliance.

D) As a security measure, details on the use of remote access and related procedures and exceptions that are granted will not be publicized, and are not to be disclosed to others who do not have a need to know.

E) Management in Organizational Units are required to sign a Risk Acceptance Agreement (attachment) that acknowledges that although best efforts were taken to reduce security risks, some risk remains ("residual" risk.) Units are required to formally accept these often unidentified, unspecified, and unknown risks.

F) OIT staff may from periodically require verification of these conditions by direct inspection, or by remote access and testing.

G) Other than the use of VPN as described above, permission is required for the use of "dial-up" access. Such permission will be contingent on responses provided to the following questions which comprise the "Permission to Use Remote Dial-up Access" form, and may be granted on a case-by-case basis.

A request form is attached that must be used to seek permission for remote dial-in over telephone circuits (POTS).

Attachments: (a) OIT-IND VPN & Token application, (b) request form for use of a dial-up modem.

(a) OIT-IND VPN & Token application (Contact the DHMH HelpDesk for this form)

(b) "Permission to Use Remote Dial-up Access Request Form"

Date:_____ Site Name : _____

Site location:_____

Person Completing Form :_____

Permitting dial-up access is contingent on your willingness to implement certain security procedures and in some cases, to install and continue to use certain security devices.

(1) Do you have currently use equipment at your site which utilizes a modem or has dial-up access to or from it?
_____ YES _____ NO

(2) What is the operating system of the equipment utilizing this dial-up connection?
_____

(3) What business need does this dial-up access fulfill? _____
_____

(4) Are you aware of any alternatives to dial-up access (e.g. DHMH VPN access) that will meet your business needs? YES___ NO___
Comments:_____

(5) What would result from your business unit's inability to use the dial-up modem capability
_____
_____

(6) What dial-in software is being utilized on each piece of equipment that has dial-up capability?
_____
_____

(7) Does your modem/dial-up equipment dial OUT to access other locations, or do others dial into your location using this dial-up access, or do both occur?
Dial-in [ ] Dial-out [ ] Both Dial-in and Dial-out [ ]

(8) Please provide the name and contact information of all users who access your site via dial-up, as well as the contact information for any location you call using a dial-up connection.

(9) Do any of devices that use dial-up services also have a Network Interface Card or other network connection attached to them

(10) What, if any security measures do you have in place to protect this dial-up equipment now?
_____
_____

(11) If granted an exception for dial-up access, does your Director or Chief administrator of your business unit or office agree to follow OIT security requirements as a condition of exception? (If permitted, we will require a Director's or equivalent management signature on a risk acceptance document)

YES__ NO___ Comments:_____

(12) Does the Director and/or business owner agree to seek on an annual basis less risky alternatives to dial-up access, or when information systems are reviewed and/or revised?

YES___ NO___ Comments:_____

(13) Please include on a separate sheet a diagram of the portion of the DHMH LAN/WAN to which your dial-up devices will be attached. The diagram must accurately reflect the current location of devices and domains.

OIT staff may contact you to confirm these answers and seek clarification, if necessary.

Exceptions may be granted only on a case-by-case basis as directed in the DHMH IT Security Policy (02.01.01, companion document "DHMH IT Security Standards & Requirements," Rev 1, 2009, Section F,5,i)

H)) and in no way sanctions the use of dial-up equipment without the express permission of the CIO or designee for each case.

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____ _____

Title: SAR-7: DHMH Information Technology Incident Response

Policy reference: Security Incident Management & Data Loss Reporting

Scope: These requirements govern all users of any DHMH network resource. These requirements apply to all network resources which reside on DHMH local area and wide area networks, as well as to any computer system, data, or information belonging to or in the custody of DHMH whether or not this data resides on the DHMH network.

DHMH employees, contractors and vendors must meet the criteria in this document for any State issued information technology device, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

DHMH requires all network management and staff to participate to implement these requirements to address security incidents.

Requirements: It is mandatory to initiate an immediate response to information systems security incidents. If a security incident occurs, a prompt and coordinated response will limit damage, speed up the recovery process and aid in restoring service.

A formal Information Security Incident Response process is required to be implemented for suspected or verified IT system breaches which may or may not have exposed non-public information to unauthorized recipients. Reporting requirements are based on the type of information exposed: (1) Exposure of Protected Health Information (PHI) is reportable under DHMH Information Security policy and by the HIPAA Security rule governing this procedure: *164.308(a)(6)(i) Security Incident Procedures*, and must follow DHMH policy under approval 01.03.07, HIPAA Breech Reporting Standard. (2) Exposure of Personal Information (PI) is governed by COMAR 10-1301-1308; Chp.304. Contact the local manager and the business unit HIPAA Contact who will report to the DHMH Privacy Officer for assistance with these mandatory, time-sensitive reports.

A.) Definition of “Information Security Incident”
B.) Authority Directing Incident Response Procedures
C.) Incident Determination Table

A) **Information Systems Security Incident**: An information systems security incident is any event, suspected event, or discovery of a vulnerability that could pose a threat to the confidentiality, integrity, or availability of supporting systems, applications, or information. Such an incident can pose actual or potentially harmful effects on a computer system. The types of activity that are widely recognized as harmful include but are not limited to:

1) Attempts (either failed or successful) to gain unauthorized access to (or use of) an information system or the data stored on the system.
2) Unwanted disruption or denial of service.
3) Unauthorized changes to system hardware, firmware, or software, including adding malicious code such as viruses and worms.
4) Detection of the above-named symptoms such as altered or damaged files, virus infection messages appearing during start-up, or inability to log in, and more.

5) The exposure of PHI/PII resulting from an incident.

B) The DHMH Incident Response process for IT Systems is directed by the Maryland DoIT, and coordinated through DHMH CIO.

C) Reporting of loss or exposure of PHI/PII is directed by HIPAA rules and DHMH HIPAA Breach Response Policy, and various sections of COMAR.

Procedures:

D) Procedures to be followed by Management and Staff are outlined in a table below and operational details in an attachment- "DHMH Information Technology System Incident Response Protocol."

E) Using this policy and with the assistance of management, make a determination of the probable type of system or data loss: PHI or PI;

F) For PHI-related breaches follow the DHMH HIPAA Breech Response Policy LINK TBD.

G) For PI-related breaches follow COMAR 10-1301-1308 available at Maryland.gov

DHMH Incident Determination Table – Use this as a tool to help determine your response.

Category	Type	Description	Report to:
Category 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a state agency network, system, application, data, or other resource.	OIT; network security staff; your manager
Category 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	OIT; network security staff; your manager
Category 3	Malicious Code	*Successful* installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	OIT; network security staff; your manager
Category 4	Improper usage	A person violates acceptable computing use policies as defined in SAR 14- Appropriate Use	OIT; network security staff; your manager

Consider the following tables as a guide to determine impact:

Functional Impact Categories

Category	Definition	Reportable to OIT. OIT reports to DoIT	Responsible staff
None	No effect to the organization's ability to provide all services to all users	N	
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	N	
Medium	Organization has lost the ability to provide a critical service to a subset of system users	Y	Manager to OIT
High	Organization is no longer able to provide some critical services to any users (COOP activation)	Y	Manager to OIT; OIT to DoIT; OP&R to MEMA

Information Impact Categories

Category	Definition	Reportable to OIT/DoIT	Responsible staff
None	No information was exfiltrated, changed, deleted or otherwise compromised	N	
Privacy Breach	Non-public: Protected Health (PHI), Personal Information (PI) employees, service beneficiaries, was accessed/exposed, or exfiltrated	Y	PHI: Manager to HIPAA Unit Contact; Contact to Privacy Officer; PI: Manager to OIT/AAG; OIT to Privacy Officer & DoIT.
Proprietary Breach	Proprietary information, such as vendor confidential/trade craft or protected critical infrastructure information (PCII), was accessed/exposed. or exfiltrated	Y	Manager to OIT/AAG; OIT to Privacy Officer & DoIT.
Integrity Loss	Public or non-public information was changed or deleted	Y	Manager to OIT; OIT to DoIT.

Recoverability Impact Categories

Category	Definition	Reportable to	Responsible staff

		DoIT	
Regular	Time to recovery is predictable with existing resources	N	
Supplemented	Time to recovery is predictable with additional resources	Y	Manager to OIT; OIT to DoIT.
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	Y	Manager to OIT; OIT to DoIT.
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	Y	Manager to OIT; OIT to DoIT.

Attachment: (1) "Maryland DoIT IT Incident Reporting Form" 4-2010

(2) "DHMH Information Technology System Incident Response Protocol," 3-2013

Attachment: SAR-7 – DoIT/DHMH Security Incident Response Form (See also SAR-15; Incident Reporting Form)

Revised 3-2013

Agency;_____ Date;_____

Point of Contact Name;_____ Phone;_____

Incident Details - Please provide as much information about the incident as possible.

Incident Category;	Incident discovery method;
1 Unauthorized access	1 Anti-virus

2 Denial of Service 3 Malicious Code 4 Improper Usage	2 Log Audit 3 Intrusion Detection (IPS/IDS) 4 User Complaint 5 System Administrator 6 Other
Source of Incident;	
IP Address_____ Port_____ # Protocol_____ Destination;_____ IP Address_____ Port_____	
Affected Agency System; Please provide information about your affected system and the impact to your agency	
System Function (e.g., DNS, Web server etc..)	
Information exposed/lost: [ ] PHI; [ ] PI; [ ] Operationally sensitive/proprietary	
Operating System_____ Version_____ Date of Latest Updates_____	
AntiVirus Installed_____ Version_____ Date of Latest Updates_____	
Briefly state the impact to your agency;	
What was the resolution?	
Does your agency require any additional assistance from DoIT?	

Attachment: DHMH Information Security or Non-public Information loss - Incident Response SAR-7

Revised 6-2014

"DHMH Information Technology System Incident Response Protocol"

A) Procedures to be followed by Management and Staff are outlined in this attached document "DHMH Information Technology System Incident Response Protocol."

This includes information system users, system owners, system administrators, system managers, and other personnel involved in the management of information systems when a suspected computer security incident occurs involving DHMH/state information systems. This report is also mandatory when non-public information is suspected or actually exposed to unauthorized users/recipients.

1) All system users: Report all incidents. All IT System or non-public information loss incidents that are suspected, unexpected, successful (or nearly successful), or those that indicate a new vulnerability or threat source must be reported immediately to your local Network Administrator, Organizational Unit Manager and the DHMH HelpDesk as a suspected or actual Security Incident.
2) Report non-public information loss (PHI/PI) to the local manager and the business unit HIPAA Contact who will report to the DHMH Privacy Officer DHMH Office of the Inspector General, Privacy Officer upon detection or suspicion. The OIG/Privacy Officer is the recognized lead agent for the investigation of data loss or exposure.
3) Individual Users' Responsibilities: Stop all work on the computer and report the information systems security incident to the HelpDesk at 410-767-6534 and to your local Network Manager, System Administrator, and Organizational Unit Manager.
4) HelpDesk / OIT-IND Network Staff & Management Responsibility: Give immediate priority to such reports.
   a) Enter the incident into the HelpDesk database.
   b) Identify the IT system or database/data owner, system administrator, and/or system manager using the DHMH Data Systems Directory.
   c) Notify OIT-IND Network Security staff and the Information Assurance Coordinator

d) Activate a conference bridge call with the designated system security personnel.

e) Determine the factual status of the event by collecting information as directed in the DoIT document cited above or in other DHMH or State prevailing guidance.

f) If situation warrants, notify OIT-IND management, unit level and one level above unit scope of control, and the Privacy Officer, for consideration and possible response escalation.

g) The Director, OIT-IND is co-delegated to officially report such incidents to DoIT Security if time is of the essence.

h) Assure procedures are in place for addressing information system security incidents that are reported after normal business hours.

5) Local Network Management Responsibility: Quickly and briefly investigate system anomalies to determine if an information systems security incident is in progress or has occurred.

a) If an information systems security incident has been detected on a system that processes non-public information or on a public web server, notify the system owner, the systems Security Officer, and the Information Assurance Coordinator.

b) If the incident has been determined to be a non-security incident, notify the HelpDesk immediately by telephone or via email and reference the HelpTicket number, if available.

6) System Information Security Manager Responsibilities:

a) Notify the OIT-IND HelpDesk.

b) If activated by OIT, act as the co-chair and participate with members of a DHMH Computer Incident Response Team (CIRT).

c) Seek technical solutions and specialized training for personnel involved with responding to information systems security incidents.

7) Network Security Staff Responsibilities

a) In consultation with Chief, OIT-IND or Designee, and the Information Assurance Coordinator, declare an information systems security incident has occurred and activate the DHMH Computer Incident Response Team (CIRT).

b) Identify and assist in accessing/assigning resources required to support the CIRT.

c) Communicate details of the information systems security incident to the Chief Information Officer (CIO).

8) Information Assurance Coordinator Role: The IAC acts as a co-chair of the DHMH CIRT, and is co-delegated with the Director, OIT-IND to report incidents to the DoIT Security staff.

a) When the CIRT is activated the IAC is responsible for the coordination of the response and reporting processes. This includes:

(1) consulting on the mitigation and recovery activities during an incident,

(2) conducting post incident follow-up to determine if a policy or procedural violation is indicated,

(3) acting to prevent recurrence within the affected system, and

(4) assuring correction of other DHMH systems at similar risk.

(5) provides guidance to assure the integrity of all other DHMH information;

(6) coordinating the preparation of the Information Systems Security Incident Report

(7) Assisting the Privacy Officer in the conduct of all data loss investigations

(8) - submitting the Information Systems Security Incident Report to the CIO within three business days.

(9) Keeping the official log for the record of the incident and resolution.

9) Chief Information Officer Responsibilities: The CIO has the final authority on all decisions related to the management of and response to information systems security incidents.

a) Communicate the details of the information systems security incident to the Chief Executive Officer and/or other senior executives and provide periodic updates concerning the significance and severity of the threat.

b) Determine appropriate level of information to release to the user community or to the DHMH Public Information Officer for public release. Release of information must be consistent with applicable Federal and State regulations.

10) Computer Incident Response Team's Membership. The actual personnel composition of the Computer Incident Response Team (CIRT) will vary depending on the event but will include personnel representative of the affected systems:

a) System Administrators,

b) System Managers,

c) the Information Assurance Coordinator and the Network Security Manager who serve as co-chairs and select the CIRT participants,

d) the team who serve as computer security subject-matter experts, which may include system administrators, network operations personnel, system security officers, ISD staff, the HelpDesk staff, and a core group of system representatives called in for each of the involved platforms.

11) Computer Incident Response Team's Duties: Follow DoIT directives if a conflict occurs within these procedures.

a) Identify and document the nature of the information systems security incident.

b) If declared a non-incident, notify the HelpDesk.

c) If declared an information systems security incident: Provide instructions to end user(s) concerning continued use of the affected system.

d) Identify whether other systems have been compromised.

e) Determine if a crime is suspected that warrants report to the AAG and police authority.

f) Formulate a corrective action plan to contain, eradicate and recover systems and data.

g) Assign a priority level sufficient to ensure the availability of any required resources. Resources must be dedicated solely to the investigation until the incident is resolved and the CIRT has been deactivated.

h) Prepare detailed documentation of information systems security incidents, including the date, time and summary of the events and a description of activities invoked by the intruder (or malicious code) as well as the actions taken to resolve the incident.

i) Document time and effort and the costs associated with resolving the current incident.

j) Submit prompt status reports as well as the information required for the IAC to complete the Information Systems Security Incident Report to the Chief Information Officer.

k) During containment, eradication and recovery:

l) Follow current DoIT/State SOP for Electronic Evidence Handling (consult with the AAG if a crime is suspected)

m) Use approved information capture techniques of pertinent files within the first ½ hour of any incident investigation.

n) Back up files, if required.

o) Secure and protect the affected system(s) and all related media.

p) Identify known risks to systems or data including any significant operational impact caused by the information systems security incident. Continue reviewing, reporting and mitigating the incident until it has been resolved. Reduce and eliminate risk and clean up the affected system. Monitor the Conference Bridge, monitor recovery process, maintain documentation, and communicate progress results to senior management.

q) Notify the HelpDesk and systems staff when the incident has been resolved.

r) Close the HelpDesk ticket.

s) Assure documentation is provided to the IAC for CIRT file record.

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Revised 3-2013

Title: SAR-8: Data Eradication Requirement

Policy reference: Device & Media Controls

Scope: This governs agency actions for all information storage media or devices containing data or information owned or in the custody of DHMH. DHMH employees, contractors and vendors must comply with the requirements and procedures outlined below.

To eliminate the possibility of inadvertently releasing residual representation of State data, State business unit will physically remove all hard drives when permanently relinquishing custody of IT equipment. The removed hard drives may either be re-used within an agency after conditioning or sanitizing as described in the SAR reference below, or must be physically destroyed such that they are permanently rendered functionally useless with data unrecoverable.

Business Unit Directors or equivalent top-level management is responsible for the hard drive removal, recycling, destruction and/or disposal process.

For situations in which the IT equipment leaves the custody of the business unit temporarily, such as servicing of equipment, a temporary loan of equipment outside of DHMH, or equipment trade-in or warranty swap, the Business Unit shall conduct an assessment of the information stored on the equipment and appropriately secure the information such that the unauthorized disclosure or use of the information is prevented. If the equipment contains confidential or high-risk information, the Business Unit shall remove the hard drive. If removal of the hard drive is not feasible, the Business Unit shall sanitize the equipment or encrypt the information commensurate with the assessment of the information contained on the hard disk.

Units are encouraged to make warranty replacement arrangements in advance with vendors who typically require the return or swap-out of apparently "defective" storage devices to assure the failed devices can remain in state custody for destruction, or be returned to the vendor in a condition that assures data cannot be recovered from the device.

Media & Devices include but are not limited to:

- Removable media
    - Memory fobs, sticks or cards
    - Magnetic disks and tapes in any form e.g. floppy disks, tape cartridges etc.
    - Optical media e.g. CDs and DVDs and similar media
- Hard drives or other memory cards/storage media in:
- PCs and Laptops/tablets;
- Personal Digital Assistants (PDA);
- Tele-comm equipment e.g cell phones, advanced communication equipment (Voip, radio, PBX, voicemail etc.;
- Fax machines, Multi-function devices (print/copy/fax);
- Process control equipment e.g. lab diagnostic machines, environmental and security systems;
- Access control/identification devices containing personally identifiable information in a directly readable or easily recoverable format, or images of clients and employees;

Requirements: (Note: desktop shredding of optical media may be personally hazardous)

DEVICE	INTERNAL REUSE	DISPOSAL	CONTACT
Hard drives *(see special considerations for solid state memory- DoIT)*	f-disk, reformat and reinstall OS. (a NIST or DoD approved sanitization software may be used)	Destroy drive by shredding or physically damaging the drive to assure data cannot be recovered.	Data Media Destruction Contact – 410-767-6830
Removable media			
Memory fobs, sticks or cards	Reset to factory status using a hard reset or unrecoverable deletion	Reset to factory status using a hard reset or unrecoverable deletion; OR Destroy by shredding	
Magnetic disks and tapes in any form	Erase using a degaussing device or overwrite procedure as specified by manufacturer.	Destroy by shredding (vendor)	
Optical media e.g. CDs and DVDs	N/A	Destroy by shredding (vendor)	Data Media Destruction Contact – 410-767-6830
PDA/cell phones	Reset to factory status using a hard reset.	Reset to factory status using a hard reset.	DHMH Central Services.
Entertainment devices (e.g. iPods®, cell phone-player combinations etc.)	N/A*	N/A*	**These are not permitted to be used or to contain DHMH data!**
Combination/Copy/Fax machines	Eradicate hard drive following manufacturer's directions or replace hard drive.*	Shred hard drive prior to machine leaving DHMH control.*	* Contact Copy, fax vendor ,machine leasing/service company prior to any action.
Access control/identification devices-badges, tokens etc.	Return to issuing authority.	Return to issuing authority or shred.	DHMH Central Services or DGS
Print device ribbons	N/A	Shred	

Procedures:

When a determination has been made to send devices as defined above to disposal or re-use the following steps are required by all DHMH business units and entities to meet the Requirements:

1. Administrative staff shall notify the business unit's network or PC staff.
2. Administrative or management staff will inspect the device to determine if any data contained on the device is required to be retained under the Business Unit's or the DHMH Record's Retention Schedule. Staff will refer to the DHMH Records Retention Document on file with their local management.
3. Business unit manager will assure records to be retained are provided to the Business Unit's Record's Manager.
4. Business unit manager will determine/approve the disposition of the device destroyed or re-used) and take the appropriate action as directed in the above requirements.
5. Property Accountable Staff shall process through DGS or other designated approving authority and document the disposition process (e.g. destruction, f-disk, reformat etc) in the Business Unit's Inventory records and retain them for audit.
6. When equipment is re-used, IT Staff shall document on the surplus property or inventory control forms the details of the drive/media initial disablement by the Business Unit, the date, device serial number, the PC or server from which the storage device was removed, if any, and signed by the staff person who performed the task.
7. Hard drives must be removed by the Business Unit. These may be sent with the related PC or server to Central Services for disposal (201 West Preston Street) hard drives must be prominently labeled or permanently marked with the (a) manufacturers serial number, and (b) the DHMH inventory number of the parent device from which the drive was removed, and (c) the name and contact information of the DHMH Business Unit.
8. NOTE: Equipment sent to Central Services with un-removed hard drives will be returned to the Business Unit.
9. Units considering outsourcing the hard drive removal and destruction shall consider the cost and the following minimal due diligence:
    - Reviewing an independent audit of the disposal company's operations;
    - Obtaining information about the disposal company from several references or other reliable sources;
    - Requiring that the disposal company be certified by a recognized trade association or similar third party;
    - Reviewing and evaluating the disposal company's information security policies or procedures; and
    - Taking other appropriate measures to determine the competency and integrity of the potential disposal company;
    - Requiring a performance bond; and
    - Requiring certificates of destruction which lists the devices and pertinent tracking information for audit purposes.

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO
Signature:	_____

Title: SAR-9: Laptop and Mobile Computing Requirements

Policy Reference: Device & media Controls

Scope: Personnel, Data, and Equipment. All DHMH Administrations, Facilities, Local Health Departments, our State agency or private partners, contractors and their sub-contractors, and volunteers, are directed to follow this Requirement to assure continued security protection of valuable, high-risk DEVICES, and confidentiality, integrity, and availability of Non-Public Information, here-after NPI. NPI includes Protected Health Information (PHI), and Personally Identifiable Information (PII).

Requirement: This Requirement comprises the minimum level of effort recognized by the Department as due diligence in the use, transportation, storage and care of: (1) a portable or "off-site" computing DEVICE as defined below, (2) the non-public data or information on them, or (3) DEVICES which facilitate access to (a) systems containing non-public information as defined below, and (b) critical Command & Control Communication and information systems.

For the purpose of the Requirement “DEVICES” shall include

- Workstation computers,
- laptops,
- personal digital assistants (PDAs),
- stand-alone or combination cell phones, radios, and digital processing equipment, and their
- related Storage Media (for the purpose of this Requirement e.g. disks, tapes, memory fobs, storage cards,) and
- any other data storage equipment, memory, or media.

This includes DEVICES (regardless of ownership) connected to or communicating with network resources, DHMH local area and wide area networks, as well as those containing Non-public information, hereinafter NPI as defined below, belonging to or in the custody of DHMH.

For the purpose of this requirement NPI includes:

Protected Health Information (PHI) as defined under federal HIPAA regulations and the Maryland Medical Records and Privacy Act,
Personally Identifiable Information (PII) as defined in COMAR: 10-1301-1308; Chp304, and
Proprietary Information as defined in COMAR,
Operationally sensitive methods regarding strengths and procedures,
Personal contact information,
Access and operational codes contained in or providing access to critical command & control communication, and related information and communication systems.

Note: This requirement replaces DHMH Directive “STANDARD OPERATING PROCEDURES (SOPs) FOR THE USE OF LAPTOPS/PORTABLE & OFF-SITE DATA PROCESSING EQUIPMENT.”

The following are considered to be the minimum level of protection required.

G.) General Care of DEVICES
H.) Locking of Devices Required
I.) Protection While Not in Use
J.) Approval for Use with NPI Offsite Required
K.) Protect Data Contained on the Devices
L.) Report Theft/Loss of DEVICES
M.) Termination/Check-Out Procedures
N.) Sanction for Failure to Comply
O.) Agreement Form & Checklist

General Care of DEVICES - DEVICES containing NPI may be used at Department and off-site locations only if an appropriate level of care is exercised equal to the risk of loss or disclosure, and written permission is granted as directed within. Users are responsible to assure that DEVICES are:

Protected **at all times** from theft attempts during times of use,
Operated, maintained and stored according to the manufacturer's and supplier's guidelines,
Stored when in transit, or not in use, in such as manner that makes it difficult for others to gain either physical or operational access to it, and
Accessed only by authorized personnel.

Locking of Devices Required – DEVICES will not be left unattended in an unsecured condition at any time. Appropriate tethers or other locks that meet manufacturers or suppliers specifications are required to be attached to an immovable object when such DEVICES are susceptible to loss by theft. The use of security equipment is considered to be a key part of due diligence in the custody of DEVICES.

Protection While Not in Use - When not in use, DEVICES must be locked in a storage cabinet, desk drawer, or a storage closet under the user's control. If there are no other reasonable alternatives, a DEVICE stored for a short period in an automobile must be out-of-sight and locked to a non-removable part of the vehicle.

Secure storage is defined as a locked metal storage or filing cabinet. The key code number, if present on the lock, shall be noted in a secured file, and then removed or erased from the lock. Appropriate key custody and security shall be followed to assure access to the storage unit is appropriately limited. This requires such keys to be under locked control at all times.

Approval for Use of State or Personally Owned Equipment and/or Permission to Process NPI Required – NOTE: DHMH and State I.T. Security Policy prohibits the use of employee-owned equipment for state business unless specifically approved by the CIO in writing for work-related use and with OIT support limited to OIT-installed applications. Processing, storing, or removal from State controlled property or equipment, or remote transmission of NPI also requires previous written approval for such use by an appropriate supervisor.

Various Federal, State, and the DHMH IT Security policy prohibit the removal of NPI from State property without the express written permission of the Custodian or Designated Responsible Party that may exceed the requirements of this Requirement.

The checklist "System/DEVICE Security Certification Checklist," (below) is to be completed in coordination with the Unit Network Manager, and approved by Organizational Unit Director in concurrence with the DHMH CIO.

The completed, approved checklist may serve as this official permission, and is required to be on file with the DHMH Information Assurance Coordinator before such use, or the issuance of a Laptop Property Pass at locations where such a pass is required by the Maryland Department of General Services (DGS).

Protect Data Contained on the Devices – Prevent theft of NPI information by using a combination of the following:

The use of one of the following OIT-approved methods is required:

i) A biometric access control that prevents access to the DEVICE and encrypts stored files, **OR**
ii) A utility that enforces and manages the use of strong passwords, file encryption, and may also provide DEVICE security tracking and recovery.
NPI on removable media must be protected by appropriate logical access controls (biometric or strong passwords) and encryption.

i) An OIT approved encryption scheme must be used to protect data on removable storage DEVICES. NOTE: Encryption schemes might not protect the data if the system is stolen while in-use mode, if the encryption is weak or the selected keys are easy to determine, or if password or encryption information is written down and attached to the unit. To assure authorized recovery of data if passwords or access codes are lost or corrupted, precautions must be taken for encryption key and password recovery by supervisors.
ii) Backup copies of NPI on removable media (tapes, hard drives, optical media, or other storage device) must be receipted, transported in an approved locked carrier by a courier under state contract, and stored in an OIT-approved off-site facility.

Data eradication steps (not simple file deletion) are required to assure data storage media are purged of all files created during work sessions and prior to the reuse or discard of the media. Follow Data Eradication Requirement SAR-8.

Clearly label all storage media that contain NPI so as to be readily distinguishable from general media. E.g. bright colored media or media storage covers.

Keep the DEVICES in physical contact when using all modes of public transportation, and be aware that typical laptop carrying cases are obvious targets.

iii) Hand carry laptops on-board aircraft
iv) Take special care during security examinations that require temporary physical separation from the system.
v) Never place yourself in danger to protect data or DEVICES. Surrender DEVICES immediately to a robber.

NPI transmitted in remote sessions e.g. email and data interchange, must be protected by locking the file at an application level, or through data encryption during transit by an approved method. e.g. SSL, HTTPS, S-FTP, VPN etc.

Theft/Loss of DEVICES- An immediate report to your Director (within 2 hours) shall be made upon the discovery of the theft, loss, or unaccountability of DEVICES containing any Department data.
If PHI/PII were contained on the DEVICE, also immediately contact the DHMH Information Assurance Coordinator (410) 767-6830.

Termination/Check-Out Procedures: At separation of employment , or if a change in job duties makes this agreement unnecessary, all employees, vendors, or agents who have completed the "**System /DEVICES Security Certification Checklist**" form will counter-sign the original and date the document when returning the DEVICE with a copy to Information Assurance Coordinator.

Sanctions for failure to comply: Any employee in violation of this requirement may be subject to disciplinary action, including bearing the replacement cost of the DEVICE, and up to and including termination of employment.

These requirements and the procedures in the attachment are intended to be in accord with COMAR and other State property procedures and requirements.

Procedures: Complete the attachment per instructions.

Attachments: "System /Device Security Certification Checklist"

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO
Signature:	_____

Attachment to Laptop and Mobile Computing Requirement: SAR-9

System /Device Security Certification Checklist

Revised 5-11

DHMH OIT

Note: Special requirements are identified by * if the DEVICE contains Non-public Information (NPI), is personally owned, or has access to State command and control systems.

In accordance with DHMH Information Security requirements, all items must be completed on this checklist. Please consult with your local network administration staff to jointly complete this form, sign and date, and provide to your local business unit Director for approval and signature. All DEVICES and procedures are subject to spot-check audits by authorized state personnel.

Signing this checklist constitutes your agreement to comply with all applicable provisions of DHMH & State I.T. Security Policy and Requirements.

Your agreement includes releasing DHMH staff from all liability related to any damages to your personally owned device- if herein approved for business use- resulting: (1) during the course of or by the installation or maintenance of business applications required by OIT for your access to State resources, or (2) from operation or access through the network.

User_____ Date_____

UNIT ADMINISTRATOR: Please keep this document in user local Personnel file.

NETWORK MANAGER: Please verify and provide the state inventory tag _____

	Required Security Practices Checklist	YES	**NO**
1	a. Is the DEVICE state equipment?		
	b. Is the DEVICE personally owned? (If personally owned, Supervisor must request permission from DHMH CIO to use for work related activities – this approval will include OIT support only for OIT-installed applications on the device.)		
	c. Is the user hereby authorized to possess and transport off of state worksites		

	Protected Health- or Personally Identifiable– Information (PHI/PII) on DEVICES listed on this form? If Yes – Make certain to complete mandatory items marked with * *(NOTE: STATE CENTER STAFF OR VISITORS CARRYING A LAPTOP ONTO DGS-CONTROLLED PROPERTY)* d. Has a DGS Police Property pass been issued to this user?		
2	If this Device has access to a Critical Command & Control Communication/Information System, or is an off-site workstation/laptop:		
	a. Is this Device protected with a BIOMETRIC access control software that controls access to the DEVICE and encrypts stored information? **OR**		
	b. Has an OIT approved software program (e.g. Dell Data Protection) been installed that enforces strong machine or file-level password access and file encryption? (Administrative Password setup and User-level/ Windows passwords?)		
3	Will auto-completion be defeated to prevent passwords from being stored in memory on this Device?		
4	Will only authorized, properly licensed, work related software packages be used on this DEVICE?		
5	When sent to disposal or re-used, will memory storage media or data contained on this DEVICE be properly eradicated or destroyed?		
6	Are backup procedures implemented automatically on an appropriate (daily/weekly) basis for this DEVICE and are these backup files maintained securely at an OIT type-approved offsite location?		
7	(a) Is a virus scan protection program automatically initiated upon boot-up on this DEVICE?		
	(b) Is an anti-spyware program used on this DEVICE?		
	(c) Are the anti-spyware and virus signatures automatically updated daily as a minimum, or more frequently?		
	(d) If this DEVICE has access to the public Internet, hardwired or through wireless services, has the Network Manager configured it securely to reduce risks associated with Internet use? (This includes the implementation of a software or hardware firewall.)		
	(e) Are auto-updates for the Operating System and key Applications on?		
8	Has the primary user of this DEVICE signed the Combined Acknowledgement Form		

	agreeing to abide by the applicable DHMH policies? (verify a signed copy is on file)		
9	a. Is the level of protection and security provided for this DEVICE the same or higher than that provided for office-based DEVICES? b. c. Are appropriate physical and point-of-use precautions in place at the worksite and off-site to prevent theft of this DEVICE?		
10	* Are PHI/PII on removable media or DEVICES containing PHI/PII protected with DEVICE access controls, or are the files password-protected at the application or encrypted at rest?		
11	* Are strong password enforcement, file/folder encryption, and optional security tracking and recovery software installed on this DEVICE? (e.g. software that can assist the police to identify a stolen Device's location.)		
12	* Has the user signed this agreement?		
13	* Does the user agree that PHI/PII will not be transmitted over the Internet without security precautions of password locking at the application or file level or transmission encryption?		
14	* Has the Business Unit Director approved this usage and signed this agreement?		

_____ _____ _____ _____

User **Business Unit** **Date** **Contact Telephone**

_____ _____ _____

Network Manager **Date** **Contact Telephone**

_____ _____ _____

Unit Director **Date** **Contact Telephone**

NOTE: Unit Administrator: If the DEVICE contains PHI/PII or is personally owned, send an original signature copy for approval to: DHMH CIO, 201 West Preston Street, Baltimore, Room 401c, MD 21201 Attention: Laptop Approval Form

Version 2 – March 19, 2013

CIO APPROVAL VERSION

In accordance with State IT Security Policy, 3.0, agency CIO must concur and approve this use.

Approved Disapproved

_____ DHMH CIO Date_____

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Revised 3-2013

Title: SAR-10: Encryption Implementation

Policy Reference: Device & Media Controls

Scope: These Encryption Implementation requirements govern all users of any DHMH information resource. These requirements apply when encryption is mandated to protect non-public data or information at rest or in transit within the DHMH infrastructure, or within a vendor-provided solution.

NOTE: DHMH and State I.T. Security Policy Section 9.4 prohibits the use of employee-owned equipment for state business. Processing, storing, or removal from State controlled property or equipment, or remote transmission of Non-Public Information requires previous written authorization for such use by an appropriate supervisor.

Requirements: DHMH employees, contractors and vendors must meet these Requirements and follow these Procedures for any State issued information technology device, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

Based on risk as determined by the system owner, custodian, or DHMH management, users shall implement appropriate levels of protection for both public and non-public information to assure its confidentiality, integrity, and/or availability commensurate with risk of loss or disclosure.

Data encryption (cryptography) is to be used in various applications and environments to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft.

Communication security (e.g. VPN, SSL, IPSEC or similar approaches) is to be used to provide protection to data by enciphering it at the transmitting point and deciphering it at the receiving point.

Based on assessed risk, file-level security is to be used to provide protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium.

Any employee in violation of this requirement may be subject to disciplinary action, up to and including termination of employment.

In the absence of specific direction from other State or Federal authority the following are to be implemented regarding encryption technology and application within DHMH.

A.) FIPS 140-2 governs the DHMH standard
B.) NIST validation of an encryption module is required
C.) DHMH required to use certain key lengths and approved algorithms
D.) Export controls extend to DHMH users
E.) Encryption to be Authorized
F.) Google Postini Encryption is the standard for email encryption
G.) Non-public Information must be protected
H.) Minimum Internet Communication Requirements
I.) Application Systems to Use DHMH-Approved Encryption
J.) DHMH VPN approved

K.) File Encryption required at rest
L.) Certificate Authority/ Key Escrow Authority established
M.) Key Recovery System Required
N.) Rogue Encryption blocking
O.) Threat scanning required on plaintext
P.) Associated costs are system owner's

A) Cryptographic modules used in DHMH will conform to the requirements of FIPS 140-2. The algorithm specified in this requirement may be implemented in software, firmware, hardware, or any combination
B) Implementations of the algorithm which are tested and validated by NIST will be considered as complying with the requirement.
C) All State computational resources using encryption shall use approved encryption algorithms and key lengths. (128 bit SSL, or AES – Advanced Encryption Standard). Unless otherwise permitted in this Requirement, the use of non-FIPS 140-2 compliant proprietary encryption algorithms is not allowed for any purpose.
D) Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations, Parts 120 through 128. DHMH will comply with these requirements and those contained in other federal and/or state law regarding export or transfer of such property or knowledge to unauthorized individuals.
E) Unless otherwise permitted in this requirement, the DHMH CIO must authorize in writing any data or voice/data encryption scheme in advance of such implementation. Only authorized users can send and receive encrypted communications. This includes individual users and peer-to-peer encryption processes.
F) The requirement for email encryption is the implementation of the proprietary encryption provided by Google Apps for Government administaered by DoIT.
G) Non-public (Protected/Proprietary) information will not be physically transported on removable media or transmitted over the public Internet without protection by either:
    i) Application-level encryption or password protection. Using a password to lock a document then attached to an email and sharing the password using another means e.g. telephone or regular mail or in person.
    ii) File encryption software – Using an approved software/hardware solution to encrypt a file when placed on removable media or attached to an email.
H) Internet encrypted communications implementation must include:
    1) adequate encryption (size and implementation scheme),
    2) employment of authentication or identification of communications partners, and
    3) a management scheme to incorporate effective password/key management systems that follow DHMH password Requirement Appendix C,
    4) the use of 128 bit SSL (https) technology as a minimum for information (communication) protection over the public Internet as transport level security,
    5) the use of WS-Security and/or ebXML are recognized to provide message level security for web services. WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. EbXML security requirements are defined elsewhere and include message security, message encryption, digital signatures, ebXML payload protection, and schema validation.
I) The implementation of private/shared key or public key encryption methods are encouraged to protect DHMH information in application systems. Consult with OIT for further information and assistance with such implementation.

J) The DHMH Virtual Private Network (VPN) is the single, authorized remote access vehicle into the DHMH WAN/LAN which provides the appropriate level of data encryption.
K) File Encryption at rest is required for non-public information when on removable media, and/or when the risk of disclosure or loss of control is determined by the custodian, owner, or DHMH Management to warrant encryption.
    1) Based on application, such file protection may also be necessary to protect the integrity of public information.
L) The Certificate Authority and Key Escrow holder for DHMH is the Director, Infrastructure & Network Division (OIT-IND), unless otherwise delegated by the CIO.
M) All encryption systems used by DHMH must have a working key recovery and custody scheme or an OIT-approved administrative procedure to protect against individual loss of an encryption key.
N) File transfers or email messages determined to be unauthorized and/or using unapproved algorithms, keys and certificates will be blocked at the DHMH/Public boundary points and disciplinary actions may be taken.
O) Plaintext (decrypted) files are to be scanned for viruses and other malicious code by the decrypting host.
P) Costs associated with general application systems development and their encryption components will be at the expense of the organizational unit/system owner.

Procedures: None

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Revised 3-2013

Title: SAR-11: Wireless Networks

Policy reference: Device & Media Controls

Scope: DHMH Wireless Network Connectivity Standard Guidelines govern the installation, operation, and monitoring of any radio frequency wireless access to any Local Area Network (LAN) which maintains a physical or logical connection to the DHMH Wide Area Network (WAN).

Requirements: Compliance with the Procedural Requirements outlined below is required by all DHMH sites. Any site with a wireless network connection which was installed prior to the issuance of these Guidelines must be brought into full compliance with these Standards within 60 days of this document's publication. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Agency CIO (or similar delegated Agency authority) are approved for connectivity to agency networks.

Procedures:

A.) Planning and Pre-Installation Procedures

B.) Installation Procedures

C.) Post Installation procedures

A.) Planning and Pre-Installation procedures

1.) Submit completed *Wireless Access Connection Proposal* (see attachment "**Wireless Access Connection Proposal Form**") to OIT-IND at least 90 days prior to anticipated installation date

2.) Wireless network access to any DHMH LAN or DHMH WAN location may not be installed or implemented without the prior written approval of that location's *Wireless Access Connection Proposal* by OIT.

B.) Installation procedures

1.) All default passwords must be changed to comply with the State of Maryland and DHMH password policies before production implementation

2.) The Secure Set Identifier (SSID) must be changed from the factory default before production implementation

3.) The beacon interval that announces the existence of a wireless network should be set to its highest value

4.) Disable the broadcast SSID feature and place the access point to minimize broadcast beyond the physical perimeter of the building.

5.) Change default cryptographic keys and use extended ASCII set where possible for complex key composition.

6.) If SNMP is not required, the local site should disable it. If SNMP is required, sites must use SMNPv3 or higher.

7.) Dynamic Host Control Protocol (DHCP) should be disabled and static IP addresses should be used on the wireless network, if feasible. IP addresses for access points and client devices must be valid DHMH routable addresses provided by OIT.

8.) The access point must verify the identity of the wireless device (i.e., open-system authentication is prohibited)

9.) Use secure access point management and assure the access point provides mutual authentication (i.e., the wireless device must authenticate the access point and vice-versa)

10.) Disable telnet services on access points.

11.) Current documentation and diagrams of the wireless network access system, as well as configuration information must be maintained in a secured location by the local network administrator and submitted initially, as well as on demand to the Director of OIT-IND Network Staff personnel or other State of Maryland personnel who have OIT-IND prior authorization.

12.) Backups of any secure and/or sensitive data accessible from the wireless network access system must be created and maintained on a regular basis. Local administrators and business owners should determine the proper frequency of these backups and the method of secure storage.

13.) Periodic security testing of all wireless network access systems must be performed at least twice a year. Documented results of these security tests must be maintained in a secure area at the local site and provided to OIT-IND Network Staff personnel upon request. OIT-IND Network staff personnel may visit a local site to perform security testing on any wireless network access system at any time

14.) Local Network Administrators must implement configuration/change control and management to ensure that equipment has the latest software release, including security enhancements and patches to discovered vulnerabilities.

15.) Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available. Local network administrators must monitor the wireless industry for changes to standards that enhance security features and for the release of new products. Counter measures such as strategically locating access points, ensuring address filtering and the installation of antivirus software must be implemented.

16.) All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

17.) Access Points / Base Stations deployed to provide Internet-only service shall be separated from the internal network by denying all internal services. Access Point / Base Station management shall be limited to internal or console users and not available to wireless clients.

18.) Wireless network access points must be physically secured with access restricted to authorized individuals only. Power buttons, reset buttons and switches must also be secured from unauthorized use.

19.) Any loss of wireless devices, security breaches and/or other compromise of existing network data or equipment that is caused or potentially caused by the wireless network access system must be reported to the DHMH Help Desk within 2 hours.

20.) IP addressing

C.) USERS

1.) Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services.

2.) Require wireless users to utilize encrypted data transmission if accessing internal LAN services.

Attachment: Wireless Access Connection Proposal Form

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO
Signature:	_____

Attachment to SAR-11: Wireless: Wireless Access Connection Proposal Form

Wireless Access Connection Proposal Form

Site Name: _____

Name of Wireless Project: _____

Person Responsible for this Project: _____

Date of Proposal Submission to OIT-IND: _____

Planned Date of Deployment for this Project: _____

1 - Describe your business need that will be met by installing a wireless access connection. List other alternatives that were explored and why those alternatives are not feasible.

2 - Identify who will be utilizing the wireless access connection at your site. Are these users State employees, Locality employees, contractors?

3 - What services, application and/or data will be accessed by this wireless access connection? What type of data will be traveling across this wireless access connection (any individually identifiable health information)?

4 - Specifically, who will install and configure the wireless equipment at your site?

Using the requirements provided above:

5 - Describe how physical access to the wireless access points will be limited? Where will the access points be placed? How will they be secured? Who will have physical access to the area where these access points will be located?

6 - In very specific detail, explain the standard security settings that you will employ on this wireless access connection. (Please make sure the 8 items from the “Standardized Configuration” requirements are met).

7 - Describe your plans and procedures that will be utilized on the wireless clients to minimize the threat they pose.

8 - Explain the guidelines that you will employ for encryption use and key management on this wireless system.

9 - How often will security assessments be performed on this wireless access connection after it is installed? What is the scope of the security testing that will be periodically performed on this wireless access connection? Who will be responsible for ensuring these security assessments are completed on a regular basis?

10 - Attach a sample copy of the configuration to be installed on the wireless equipment

11 - Attach a detailed diagram (in Visio format) of the proposed wireless access connection's physical and logical layout.

12 - Attach a detailed catalogue of the hardware components to be used in this proposed wireless access connection. Include band names, model numbers, and software release versions.

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Title: SAR-12: Password Requirements

Policy reference: Access & Authorization

Scope: This requirement governs all network administrators, developers and users of any DHMH network resource. The requirement applies to all network resources which reside on DHMH local area and wide area networks, as well as any computer data belonging to DHMH whether or not this data resides on the DHMH network.

Requirements: DHMH employees, contractors and vendors must utilize passwords which meet this criteria for any State issued information technology device, account and/or access, as well as any non-State issued account/resource on which State data or work product stored or processed.

For DHMH network administrators, strong passwords must be utilized for access to server administration accounts, email administrative accounts, server screensavers and network infrastructure equipment (hubs, switches, wireless access points).

Application developers must ensure their programs meet the criteria outlined in these standards.

Basic Password Standards- Implement the following to assure passwords must meet the following construction, usage and change requirements:

- The password must not be the same as the user id;
- Passwords must not be stored in clear text;
- Passwords must never be displayed on the screen;
- Change temporary passwords at the first logon;
- Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters;
- Passwords must not contain leading or trailing blanks;
- Automate required password change at regular intervals;
- Password reuse must be prohibited by not allowing the last 10 passwords to be reused with a minimum password age of at least 2 days;
- Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
- Passwords older than its expiration date must be changed before any other system activity is performed;

- User IDs associated with a password must be disabled after not more than four (4) consecutive failed login attempts while allowing a minimum of a ten (10) minute automatic reset of the account;

- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

Procedures:

A.) Network User Responsibility
B.) Network Administrators Responsibility
C.) Application Developers Responsibility
D.) Strong Password Construction Guidelines
E.) Weak Password Characteristics
F.) System-level Password Requirements
G.) Password Protection Practices
H.) Remote Access Guidelines
I.) Pass-phrases

A.) Network User Responsibility

1.) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.

2.) Passwords are never to be inserted into email messages or other forms of electronic communication except when system-generated and provided as a one-time “reset” password requiring user change on next login.

B.) Network Administrators Responsibility

1.) All system-level passwords (e.g., root, enable, admin, supervisor, Administrator, application administration accounts, etc.) must be changed at least every 45 days.

2.) User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

3.) Where SNMP is used, the community strings must be defined as something other than the default "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available .

C.)Application Developers Responsibility

1.) Applications should support authentication of individual users, not groups.

2.) Applications should not store passwords in clear text or in any easily

reversible form.

3.) Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.) Applications should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D.) Strong Password Construction Guidelines

1.) Contain both upper and lower case characters (e.g., a-z, A-Z).

2.) Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~- =\‘{}[]:";’<>?,./).

3.) Contains at least eight characters.

4.) Must not contain leading or trailing blanks.

5.) Must not contain more than 2 consecutive identical characters.

6.) Must not be identical passwords to old passwords used within the past 6 months.

7.) Must differ from prior passwords by at least 2 characters.

8.) Is not a word in any language, slang, dialect, jargon, etc.

9.) Is not based on personal information, names of family, pets, etc.

10.) Passwords should never be written down or stored on-line.

11.) Must not be the same as the userID. (DoiT compliance 12/09)

E.) Weak Password Characteristics

1.) Contains less than eight characters.

2.) Is a word found in a dictionary (English or foreign).

3.) Is a common usage word such as:

-Names of family, pets, friends, co-workers, fantasy characters, etc.

-Computer terms and names, commands, sites, companies,

hardware, software

-The words "<Company Name>", "sanjose", "sanfran" or any derivation

-Birthdays and other personal information such as addresses and phone numbers

-Word or number patterns like aaabbb, qwerty, 123321, etc.

-Any of the above spelled backwards

-Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

F.) System-level Password Requirements

1.) Expired passwords must be changed before any other system activity is performed.

2.) User IDs associated with a password must be disabled after no more than four consecutive failed login attempts and require security administration to reactivate the ID.

3.) When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

G.) Password Protection Practices

1.) Do not use the same password for accounts at work, home or personal accounts.

2.) Do not use the same password for various access needs.

3.) Don’t reveal personal passwords over the phone to ANYONE.

4.) Don’t reveal a password in an email message.

5.) Don’t reveal a password to your boss.

6.) Don’t talk about a password in front of others.

7.) Don’t hint at the format of a password (e.g., "my family name").

8.) Don’t reveal a password on questionnaires or security forms.

9.) Don't share a password with family members.

10.) Don't reveal a password to co-workers while on vacation.

11.) If someone demands a password, refer them to this document or have them call someone in the Infrastructure/Network Division.

12.) Do not use the "Remember Password" feature of applications (e.g., Maryland.gov, web browsers.

13.) Do not write passwords down and store them anywhere in your office.

14.) Do not store passwords in a file on ANY computer system (including Smartphones or similar devices) without encryption.

15.) If an account or password is suspected to have been compromised, report the incident to OIT-IND HelpDesk (410-767-6534) and change all passwords.

H.) Remote User Access

1.) User access to the DHMH networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass-phrase.
2.) All VPN remote access to any part of the DHMH network will utilize some form of an authentication token or automated certificate presentation.
3.) OIT-IND is the only entity in DHMH which is allowed to procure, administer and maintain any type of remote connectivity or token-based authentication system to the DHMH network.

I.) Pass-phrases

1.) Use of pass-phrases is encouraged.

2.) Are subject to the same rules listed above.

Attachments: None

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

CIO APPROVAL VERSION

Signature: _____

Revised 3-2013

Standard: SAR-13: Firewalls

Policy Reference: Device & Media Controls

Scope: The DHMH Firewall standard governs firewall installation, configuration, management and monitoring. Compliance with this standard is required by all entities within DHMH for devices connected to the DHMH LAN/WAN.

For purposes of this standard, firewalls are defined as security systems, which control and restrict the connectivity and services for Internet, Intranet, Statewide Government Intranet (SwGI), and 3rd party networks. Firewalls are further defined as any device or software that intercepts network traffic and has the ability to block or permit traffic, perform network address translation, or otherwise obfuscate DHMH routable IP addressing. Firewalls establish perimeters where access controls are enforced.

Requirements: No DHMH computer system may be attached to the Internet unless it is protected by a firewall.

Firewalls installed prior to the issuance of this standard must be removed from the network within 60 days of this document's publication. Systems not so protected must after this implementation period must be disconnected until so protected.

Firewalls must be located in physically and environmentally secure areas.

Installation - The Infrastructure/Network Division (OIT-IND) is solely responsible for firewall installations throughout DHMH. No other Administration is permitted to procure or install firewalls for their own purposes.

Configuration & Management - Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of business advantages and security risks. The agency enterprise network manager is the recognized decision maker who can either approve or deny these requests.

Requests for firewall services to be added, removed or changed must be submitted via Intranet form at http://dhmhdatacenter/fwrequests (form also attached). Requests will be reviewed and denied/approved within 7 business days. Firewall requests will not be approved unless a documented business need is identified and benefits to the Agency outweigh security risks.

OIT-IND requires Firewall rule and service requests as submitted by Business Units be reviewed by the originating unit and verified every 90 days, or as deemed necessary by OIT-

IND. Failure to validate the continuing need for the rules/services will result in rule/service suspension until verification is received.

OIT-IND has established general port rules for http/https, smtp, telnet, ftp/s-ftp, including traffic flow, and firewall traffic behaviors to control and secure network level access. All inbound connections not specifically permitted from external networks to ports and services on the DHMH network are denied. Additionally, the following must be implemented:

- Permit only documented and approved inbound traffic to non-internal host/subnets;
- Disable all unused services;
- Hide and prevent direct access to state trusted network addresses from un-trusted sources;
- Default administrator username and password must be changed;
- Management access must be limited to appropriate personnel;
- Maintain comprehensive audit logs and implement review procedures;
- Fail in a closed state;
- Operate on a dedicated platform (device);
- All devices shall have updates and patches installed on a timely basis to correct significant security flaws.
- All publicly accessible servers must be separated from any internal subnets by a firewall. Strict access control must be enforced between publicly accessible subnets and internal subnets by documented and approved access-lists.

Management - Management access must be managed and maintained by specified firewall administrators using a secure communication channel (encryption) e.g. secure shell sessions from specific source addresses from workstations specifically permitted to manage firewalls, or through a console connection.

Software updates are to be performed regularly. When known vulnerabilities are announced, updates must occur immediately.

Monitoring - Because firewalls provide such an important barrier to unauthorized access to networks, they must be audited at least annually. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures. These audits must also include the regular execution of vulnerability identification software.

All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity, which might be an indication of unauthorized

usage or an attempt to compromise security measures, must also be logged. The integrity of these logs must also be protected with checksums, digital signatures, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least three months. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Procedures: Units requesting changes to the Firewall shall complete the attached form **DHMH Firewall Rule Modification Request Form** as directed in the attachment.

Attachment: (1) "Firewall Rule Modification Form"

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

Attachment to SAR-13: Firewalls

Revised 3-2013

Maryland Department of Health and Mental Hygiene

Firewall Rule Modification Request Form

Requestor Name:_____

Administration: _____

Phone: _____

Email: _____

Date of Request:_____ Implementation Date Requested:_____

System supported:_____

Please state your business reason for requesting firewall changes:

_____

Firewall rules: (Row 1 is an example)

	Source Address	Source Port	Destination Address	Destination Port	Action	Description and Justification
1	1.1.1.0/24	any	2.2.2.2/32	23	permit	Allow telnet from any host on 1.1.1.x to host 2.2.2.2.
2						
3						
4						
5						
6						
7						

Original issue date: March 19, 2013
Last review date: June 28, 2014
Review frequency: Annual
Review by: Information Technology Governance Board
Approved: Kevin Naumann, Interim CIO

CIO APPROVAL VERSION

Signature: _____

Revised 3-2013

Title: SAR-14: Appropriate Internet and other Electronic Communications and Use

Policy reference: Appropriate Use & User Responsibilities

Scope: This document sets standards and requirements of the State/DHMH with respect to access, disclosure, recording, and general usage of electronic communications created, received, or stored through the use of the electronic communications systems owned, leased, or otherwise affiliated with DHMH.

The purpose of this policy is to explain the ownership of the electronic communications created, received, or stored on the State/DHMH electronic communications systems and to inform users of the systems about their rights and duties with respect to electronic communications.

This policy applies to users of State electronic communications systems and may be changed by the DHMH CIO, at its discretion, without prior notice. These standards and requirements for this policy are in addition to, and not in replacement of, any other published policy or code of conduct of Executive Departments and Independent State Agencies.

The State encourages the use of electronic communications and electronic communications systems to enhance efficiency. Electronic communications and electronic communications systems are to be used 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.

Requirements: These Requirements direct the appropriate use of Internet and data Communication Services as specified, including the use of Social Media for business purposes.

ACCEPTABLE USE

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.

UNRESTRICTED PERSONAL USE IS PROHIBITED of DHMH Internet and electronic communication services and systems.

Restricted Personal use means acceptable use that is not job-related. The State's electronic communications systems may be used for minor, incidental personal uses, as determined by local management that are not intentional misuses.

Personal use shall not directly or indirectly interfere with the Agency's business uses, directly or indirectly interfere with another user's duties, or burden the State with more than a negligible cost.

In general, "acceptable" means limited, incidental and occasional personal use of the DHMH Internet access or electronic communication systems is permitted. However, personal use is prohibited if such use:

- interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
- adversely affects the efficient operation of the user's workstation, servers, or DHMH LAN/WAN;
- 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.

NOTE: Users employing the DHMH Internet or electronic communication systems for acceptable personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of the agency or the State.

No Expectation of Privacy:

The State reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on the State's electronic communications systems, including minor incidental personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.

Except where security is explicitly provided to meet federal or state laws or regulations for data security, no user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the DHMH equipment and/or access e.g. financial information, credit card or account information or transactions.

DHMH has a right to monitor any and all aspects of data communications and computer systems including, but not limited to, sites, instant messaging systems, chat groups, or news groups visited by agency users, material downloaded or uploaded by agency users, and e-mail sent or received by agency users. Such monitoring may occur at any time, without notice, and without the user's permission.

The State reserves the right to access, intercept, inspect, record, and disclose any electronic communications on its systems during or after normal working hours and even if the electronic communications appear to have been deleted from the electronic communications systems. The use of a State password shall not restrict the Agency's right to access electronic communications.

Senior management or individuals with delegated authority, from Executive Departments and Independent State Agencies have the authority to determine when employee personal use exceeds minor, incidental, or inappropriate.

Authorized users are responsible for the security of their passwords and accounts. Users shall not disclose their passwords unless authorized by Senior Management in exigent circumstances because disclosure is necessary to support the business of the government.

NOTE: In addition, electronic records may be subject to the Maryland Public Information Act, and therefore, **available for public distribution, review, and publication**.

PROHIBITED ACTIVITIES/INTENTIONAL MISUSE

Intentional misuse includes, but is not limited to, receiving, displaying, storing, or transmitting threatening or sexually-explicit images, messages, or cartoons as well as epithets or slurs based upon race, ethnic or national origin, gender, religious affiliation, disability, or sexual orientation and harassing, offensive, discriminatory, or defamatory communications or images. It also includes attempting to access a secured system or database, whether private or public, without permission.

UNACCEPTABLE USE EXAMPLES

The following activities are examples of general unacceptable use of agency electronic communications:

- Engaging in any activity that is illegal under Local, State, Federal or International law in conjunction with the usage of the State's electronic communications systems.
- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.
- Unauthorized reproduction of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Agency or the user does not have a specific and active license.
- Exporting software, technical information, or technology in violation of International or regional export control laws.
- Introduction of malicious programs into the State's electronic communications systems infrastructure including, but not limited to, computer workstations, servers, and networks.
- Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others.
- Interfering with or denying electronic communications system services to any user.
- Inappropriate purposes, in violation of the intended use of the network, as defined by this policy and DHMH CIO.
- Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses.
- Effecting security breaches or disruptions of any electronic communications system. This includes, but is not limited to tampering with the security of State owned computers, network equipment, services or files, as well as any other type of unauthorized system access.
- Attempting to intercept, modify or monitor network traffic or systems, without prior written permission from the Director of OIT/IND.

PROHIBITED PERSONAL-USE ACTIVITIES

Certain activities are **prohibited at all times** when using State/DHMH information equipment, systems, or Internet or electronic communications for **personal use**. These include, but are not limited to creating, copying, accessing, attempting to access, installing, uploading, downloading, transmitting, printing, sharing, or storing:

- lengthy private messages,
- religious/faith-based or politically-related messages,
- sexually explicit information or content;
- fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;

- unauthorized computer software, programs, or executable files contrary to software copyright and use policy
- music and video downloaded files or streaming transmissions including news and entertainment, and
- Engaging in Social Media networks outside of authorized business uses.

It is also **PROHIBITED** at any time to:

- Access or attempt to access an account or information to which you are **not authorized**.
- **misrepresent** yourself as another person or entity (an example but not limited to) sending e-mail using another's identity, an assumed name, or anonymously;
- use DHMH equipment or services to endorse commercial products or enterprises, or for **personal enterprise – for profit or non-profit**;
- engage in lobbying;
- Purchase goods or services for private use;
- permit anyone other than yourself the **use of your workstation**, extending access to data or information or systems under your control, or facilitating access to DHMH equipment or services; this includes **allowing others the use State equipment in your care for personal use**, or to
- Engage in activities **prohibited** by the agency.

SOCIAL MEDIA USAGE

Social media is content created using highly accessible Internet-based publishing technologies used to share opinions, insights, experiences, and perspectives with others. These emerging collaboration platforms offer new ways for State employees to build citizen and agency relationships. Social media can also be used by State employees to take part in national and global conversations related to activities within the State. Choosing the option to utilize social media technology is a business decision. It must be made at the appropriate level for each DHMH Business Unit with regard to its mission, objectives, capabilities, and potential benefits, and risks to the agency.

The purpose of this policy is to provide rules of conduct to DHMH Business Units, employees, vendors, and volunteers when using social media technologies to engage with citizens on behalf of the State of Maryland. DHMH expects and requires all authorized participants in social media on behalf of the State to understand and to follow these guidelines.

When a DHMH Business Unit decides to engage representation on specific social media sites, the Business Unit must in memo sanction official participation and representation on specific social media sites. The agency has an overriding interest and expectation in deciding who may "speak" and what is "spoken" on behalf of the agency and of the State. If approved within an agency, social media sites are to be used for business purposes only in serving the interests of the Agency, the State, and the citizens, visitors, and commerce partners of the State of Maryland. All electronic communications created, received, or stored on the Agency's or State's electronic communications systems are not the sole property of the author, recipient, or user.

State employees and/or contractors representing the State are responsible for the content they publish on social media sites. Wherever possible, links to more information should direct users back to official websites for more information, forms, documents or online services necessary to conduct business with the State/agency.

IDENTIFICATION AND ORIGIN OF PARTICIPANT- During the use of a social media site channel on behalf of the State of Maryland, the response will either be “individual” (from a State Employee), or “organizational” (from a State Organization):

Individual, originating from a State employee conducting State business on a DHMH controlled social media site: The State Employee must disclose the following information within their communication: First and Last Name, Contact Information (at a minimum a State E-mail address must be provided - including more information is permitted), and their organization (Department or Agency Name).

Individual, originating from a State employee clearly representing themselves as a State employee publishing content to any social media site outside of a Maryland domain and not conducting state business, must use a disclaimer such as this: "The postings on this site are my own and don't represent Maryland's positions, strategies or opinions."

DHMH Business Unit, originating from a DHMH controlled social media site: The Business Unit must disclose the following information as part of their use of a communication channel: Business Unit Name and a single point of contact for inquires about the channel (at the minimum, a general E-mail address - including more information, such as the Organization’s Telephone Number, is permitted).

MODERATING COMMENTS- In some social media formats, state employees may be responsible for moderating comments. If user content is positive or negative and in context to the conversation, then the content should be allowed to remain, regardless of whether it is favorable or unfavorable to the State.

Data leakage incidents such as disclosure of non-public information, or making inappropriate public statements about or for the State/Agency, or using State resources for personal uses, and harassing or inappropriate behavior toward another employee can all be grounds for reprimand or dismissal.

ETHICAL CONDUCT- DHMH organizations will act and conduct themselves according to the highest possible ethical standards. A summary of the key points of ethical social media conduct that should be part of the Business Unit operating procedure are reproduced below. Employees and Business Units:

- shall be familiar with and comply with the terms and conditions of the social media site.
- must not knowingly communicate inaccurate or false information. All reasonable efforts should be made by the State Employee or State Organizations to provide only verifiable facts—not unverifiable opinions. We will publicly correct any information we have communicated that is later found to be in error.

- must maintain confidentiality of State of Maryland information that has been identified or is reasonably considered to be confidential and not publicly disclosable in nature.
- will respect the rules of the Social Media venue.
- will report any suspected violations or concerning materials to management for timely action.

GUIDING PRINCIPALS- DHMH Business Units developing a social media site on behalf of the state can utilize the state guidance provided at:
http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf see Section 12.0.

If your Business Unit participates in social media, it is recommended that you adhere to these guiding principles and make these conditions of use with your employees:

- Stick to your area of expertise and provide unique, individual perspectives on what is going on at the State, and in other larger contexts.
- Post meaningful, respectful comments, no spam, and no remarks that are off-topic or offensive.
- Respect proprietary information, content, and confidentiality.
- When disagreeing with others' opinions, keep it appropriate and polite
- Remain focused on customers, existing commitments, and achieving the State's/agency's mission.
- Your use of social media tools should never interfere with your primary duties, with the exception of
- where it is a primary duty to use these tools to do your job.
- Only public information can be disclosed on social media sites. Information on the Maryland Public Information act can be found at http://www.oag.state.md.us/Opengov/pia.htm

SECURE PRACTICES- There are risks associated with the use of social media. Be aware that:

- The information you post online could be used by those with malicious intent to conduct social engineering scams that attempt to steal confidential data. Be cautious in how much personal information you provide - remember that the more information you post, the easier it may be for an attacker to use that information to steal confidential data.
- Stealing passwords is a common way hackers can gain access to social media accounts. When creating an account, follow password complexity best practices and choose password reset questions that cannot be easily guessed or answered through research.
- Do NOT use the same passwords that you use for other personal or business access.
- Security technologies shall be implemented to protect State-represented social media sites from unwanted user-generated content.

TERMINATION OF ACCESS

- User's access to State electronic communications systems resources shall cease immediately when one of the following occurs:
- Termination of employment.
- Termination of a contractor's or consultant's relationship with the State.
- Leave of absence of employee.
- Lay-off of employee.
- A determination by senior management that an employee or user constitutes a threat to the DHMH network or data infrastructure.

Procedures: Units are directed to implement these requirements; personnel are required to read, agree to DHMH IT Security Policy, Standards and Requirements, and annually sign the Combined Acknowledgement Form SAR-4.

Attachments: "OIT-IND Network Use Inquiry Form"

Original issue date:	March 19, 2013
Last review date:	June 28, 2014
Review frequency:	Annual
Review by:	Information Technology Governance Board

CIO APPROVAL VERSION

Approved: Kevin Naumann, Interim CIO

Signature: _____

Attachment to **SAR-14 - "Appropriate Use & User Responsibilities"**

OIT-IND Network Use Inquiry Form

Data Collection Requestor: _____

Inquiry Subject's Name: _____

Relationship of Requestor to Subject: _____

Property Tag Number of PC to be Searched: _____

Physical Location of PC: _____

****

What are you requesting OIT-IND to search?: _____ Internet Usage _____ Email Usage

What are you requesting OIT-IND to search for data of?

	Sexually Explicit		Gambling		Personal Shopping
	Online Games		Instant Messaging		Auction Sites
	Listening/Recording Music		Watching/Recording Streaming Video		Non-Business Use of Email
	Downloading Unauthorized Software		Other (Be Specific):		

****

I affirm that I am requesting the Infrastructure/Network Division to search the above listed user's DHMH network usage. I understand that OIT-IND will supply the requested information to me only, unless data indicating possible criminal activity is found. If such information is found, I understand that it will also be turned over to the DHMH Office of the Inspector General. I affirm that I currently hold the title of at least Branch Manager and that I have authority to request data collection for this employee.

Requestor's Signature: _____ Date: _____

****

FOR OIT-IND OFFICE USE ONLY

Request received by: _____ Date request received: _____

Search Performed by: _____

Location Where Data was placed on OIT-IND Server: _____

Date of Initial Search: _____ Data Sent To: _____ Date of Turnover: _____

Date of Follow-Up Search: _____ Data Sent To: _____ Date of turnover: _____

Date of Follow-Up Search: _____ Data Sent To: _____ Date of turnover: _____

Date of Follow-Up Search: _____ Data Sent To: _____ Date of turnover: _____

Additional Action Taken With Data (if any): _____

_____

********** END OF FORM **********

SAR-15: Security Incident Response *(SAR-7)* **- Reporting Form- Rev 9/2013**

NOTE: All actual reports are to be filed
by fax to 443-926-9742 or saved as PDF and email to: service.desk@maryland.gov

Agency;_____ Date;_____

Point of Contact Name;_____ Phone;_____

Incident Details - Please provide as much information about the incident as possible.

Incident Category;	Incident discovery method;
1 Unauthorized access 2 Denial of Service 3 Malicious Code 4 Improper Usage	1 Anti-virus 2 Log Audit 3 Intrusion Detection (IPS/IDS) 4 User Complaint 5 System Administrator 6 Other
Source of Incident;	
IP Address_____ Port_____ # Protocol_____ Destination;_____ IP Address_____ Port_____	
Affected Agency System; Please provide information about your affected system and the impact to your agency	
System Function (e.g., DNS, Web server etc..)	
Operating System_____ Version_____ Date of Latest Updates_____	

AntiVirus Installed_____ Version_____ Date of Latest Updates_____
Briefly state the impact to your agency;
What was the resolution?
Does your agency require any additional assistance from DoIT?

Original issue date:	March 19, 2013
Last review date:	None
Review frequency:	Annual
Review by:	Information Technology Governance Board
Approved:	Kevin Naumann, Interim CIO

Signature: _____

SAR-16: Attachment 2: **"DHMH INFORMATION TECHNOLOGY SECURITY PROGRAM – InfoSec"**

The table provides a compact reference to the component requirements of the DHMH Information Security Program.

Required Program Element	What must be done	Who does the work	How it's to be done	Compliance measurement and date	Estimated risk of noncompliance
1. IT Security Policy Management	DHMH & Business Units must implement the IT security policy, with standards, and procedures.	CIO, CISO, Directors, LHOs, Network Managers, Users	1. CIO directed preparation of DHMH Policy, Standards, and guidelines 2. Coordinate appropriate processes with DHMH Privacy and Compliance Officer 3. Designate certain responsibilities for IT Security Program management and compliance to CISO and others. 4. Work with DHMH OIG and OLA Legislative Audit for compliance reviews	Completed and promulgated DHMH policy Business Unit compliance statement in memo by accepted date.	Formidable. Potential loss or significant reduction of federal funding for federally mandated systems if not in compliance with federal requirements.
2. Risk Management & Assessment	A risk management – *system assessment- process* must be implemented to assess the acceptable risk to DHMH IT systems as part of a risk-based approach used to determine adequate security for the system.	CIO, Directors, Network and System Managers	1. Compile list of "critical" systems (Data Systems Inventory- see 4.4) 2. Analyze threats and vulnerabilities 3. Select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. 4. Continue to hold SeCon, and InfoSec meetings to discuss agency-wide IT and Physical Security and Privacy concerns and	1. Define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system. 2. Report noncompliant systems to OIG. Compliance within X	Varies by system; potentially expensive and embarrassing, and could significantly impact public trust of health systems.

			provide recommendations to the CIO.		
3. IT Security Certification & Accreditation	Develop and implement an IT security certification and accreditation program as part of an overall IT risk management strategy.	Business Unit management, System Owners	1. Maintain a catalog of all IT systems and sites including existing 2. rank by sensitivity and criticality. 3. Follow DHMH Certification and Accreditation (C&A) Guidelines.	1. Define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system. 2. Report noncompliant systems to OIG.	Holding IT system acquisition until compliance is met
4. Systems Development Life Cycle Methodology	Enforce internally a System Development Life Cycle (SDLC) management process that includes IT security as part of the model.	CIO, Directors, Procurement	1. Use Data Systems Inventory to identify critical systems requiring SDLC process. 2. Schedule security assessment and compliance as part of the review process.	Compare completed SDLC reports to required systems list. Compliance within X Compliance within X	Holding IT system acquisition until compliance is met
5. IT Disaster Recovery Planning	Develop, implement, and test an IT Disaster Recovery plan for each critical IT system	Info Assurance Coordinator, Business Unit management, System Owners, DBAs	1. Use SDI to identify Critical Systems 2. Ensure that Business Unit DR & related IT contingency plans are in place and, 3. Test contingency plans to assure alternate to primary production system. (Reference DHMH & State IT Disaster Recovery Guidelines)	1. Define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system. 2. Report noncompliant systems to OIG. Compliance within X	Varies by system based on funding entity e.g. federal funds might be withheld for non-compliance

6. IT Security Awareness, Training, and Education	Develop and implement a security awareness, training, and education program for all agency employees and contractors.	CIO, Directors, Employees Volunteers Contractors	1. Continue to provide InfoSec website for all employees and contractors 2. Mandate Web-based IT Security Awareness Training and Education is completed 3. Provide limited Face-to-face training. 4. Implement a multi-media awareness program	1. Assure employees complete training using training system administrative tools. 2. Report noncompliant users to management for sanction. Compliance within X	Employee access might be temporarily suspended.
7. Communications & Operations Management	Develop and implement a Comm/Ops assessment and documentation process in each Business Unit.	Business Unit management, System Owners	1. Review and document required elements 2. Validate implementation	Verify compliance through reports Compliance within X	Violation citation to Business Unit manager; failure to comply triggers notice to OIG for follow up
8. Access Control	Develop and implement an Access Control assessment and documentation process in each Business Unit.	Business Unit management, System Owners	1. Review and document required elements 2. Validate implementation	Verify compliance through reports annually	
9. Critical Incident Response Process	DHMH must continue to participate in the State Incident Response Process.	CIO, OIT-IND, Network Managers Contractors	3. Assure all members named in the DHMH IT Incident Response Standard are made aware of the duties and obligations under this Policy. 4. Test the IT Incidence Response Plan annually	Compliance within X	
10. External Connection Review	DHMH must continue to review external network connections	CIO, OIT-IND, Network Managers, Business Unit management	5. Ongoing review of external connections 6. Review of non-networked computers and remote/dial-in connections shall be managed, reviewed	1. Set an annual date and schedule for each critical system to complete review 2. Results will be reported annually. Compliance within X	

			annually. 7. Assure approval and SLAs in place for all external connections		
11. Compliance IT Security Program Reporting	DHMH, CIO, is responsible for reporting on the status of the agency IT Security Program to the DoIT/OIT Security Division annually.	CIO, Directors, Network Managers, Budget Office	1. Prepare Security Program annual report 2. Must include critical system SDLC, Risk Assessment, and project plans. 3. Detail project estimated costs compliance dates.	Completed annual report to OIT Compliance within X	

Original issue date: March 19, 2013
Last review date: June 28, 2014
Review frequency: Annual
Review by: Information Technology Governance Board
Approved: Kevin Naumann, Interim CIO
Signature: _____