STATE OF MARYLAND

INFORMATION SECURITY POLICY

Version 3.1

February 2013

TABLE OF CONTENTS

PURPOSE

The purpose of this policy is to describe security requirements that Executive Departments and Independent State agencies must meet in order to protect the confidentiality, integrity and availability of state owned information. This Policy shall serve as information technology best practice for all other State agencies. Any agency, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), may exceed the security requirements expressed in this document, but must, at a minimum, conform to the security controls required by this Policy.

SCOPE

This policy applies to confidential information, as defined in section 3.1, that is electronically generated, received, stored, printed, filmed, and typed, regardless of whether the electronic system is hosted on a State network or a 3rd-party offsite premise. The provisions of this policy apply to all units in the Executive Branch of the State of Maryland and Independent agencies unless an exception has been previously approved.

AUTHORITY

The Department of Information Technology (DoIT) has the authority to set policy and provide guidance and oversight for the security of all IT systems in accordance with Maryland Code § 3A-303 and § 3A-305.

RECORD OF REVISIONS

Date	Revision Description
September, 2009	Version 2.0: 1. Major changes in document presentation and format. 2. Content based on ISO 17799: 2005 3. Increased emphasis on protection of confidential information.
September, 2009	Version 2.1: Revised Appendix A – Computer Security Incident Handling Form
October 2009	Version 2.2: 1. Section 7.8 - Added Wi-Fi certified devices only. 2. Section 8 - Revised Access Control section. 3. Section 8.1 - Added password reuse and minimum password age requirements. 4. Section 9 - Revised Communication and Operations Management. 5. Appendix B - Added Wi-Fi certified.

September 2010	Version 2.3: 1. Section 2.1 - Modified agency responsibilities 2. Section 3.1.1 – Modified policy on the storage of confidential information on portable devices. 3. Section 4.6 – Modified IT Incident Response Process 4. Section 5.3 – Added Social Media Policy 5. Section 6.4 – Modified Storage Media Disposal Policy 6. Appendix A – Added definitions 7. Appendix B – Modified reporting form
2011	Version 3.0: 1. Adopt NIST Risk Management guidelines 2. Added Solid State Drive Sanitation 3. Added DR Requirements 4. Added Virtual Technologies 5. Added Public Cloud Computing Technologies 6. Added Security Compliance tools 7. Modified password requirements
2013	Version 3.1: 1. Refined cloud guidelines 2. Added Agency responsibilities 3. Strengthened confidential information protection requirements 4. Updated Risk Management guidelines 5. Updated Security Assessment guidelines 6. Updated Security Configuration guidance 7. Updated Incident Response guidance 8. Updated Media Protection guidance 9. Updated Log Retention guidance 10. Updated guidance on disabling user accounts 11. Updated password guidance 12. Added Mobile Device Security Policy guidance 13. Added Data Loss Prevention guidance

SECTION 1: Preface

Information and information technology (IT) systems are essential assets of the State and vital resources to Maryland citizens. These assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as to local and federal government entities. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting such information from unauthorized access, modification, disclosure and destruction. This Policy sets forth a minimum level of security requirements that, when implemented, will provide the confidentiality, integrity and availability of Maryland IT assets.

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NISTs mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In general, the State of Maryland will adopt NIST information security related standards and guidelines. Security policies developed to secure an agency information system should refer to a particular NIST standard [and] agencies shall develop procedures to ensure compliance with the policy. In the event that a published NIST standard is deemed insufficient or non-existent, agencies shall adopt industry accepted security guidelines (or develop them) and refer to them within their security policy.

While state agencies are required to follow certain specific requirements in accordance with this policy, there is flexibility in how agencies apply NIST guidance. State agencies should apply the security concepts and principles articulated in the NIST Special Publications (SP) in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance can result in different security solutions that are equally acceptable and compliant. When assessing state agency compliance with NIST SP, evaluators, auditors, and assessors should consider the intent of the security concepts within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

SECTION 2: Roles and Responsibilities

The following policy sets the minimum level of responsibility for the following individuals and/or groups:

- Department of Information Technology;
- Agency; and
- Employees and Contractors.

2.0 Department of Information Technology

The duties of the Department of Information Technology are:

- Developing, maintaining, and revising IT policies, procedures, and standards;
- Providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning IT matters;
- Developing and maintaining a statewide IT master plan; and
- Adopting by regulation and enforcing non-visual access standards to be used in the procurement of IT services by or on behalf of units of State government

2.1 Agency

Information security is an agency responsibility shared by all members of the State agency management team. The management team shall provide clear direction and visible support for security initiatives. Each agency is responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy;
- Implementing and maintaining an IT Security Program;
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency security program;
- Ensuring that security is part of the information planning and procurement process;
- Participating in annual information systems data security self-audits focusing on compliance to this State data security policy;
- Determining the feasibility of conducting regular external and internal vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses;
- Implementing a risk management process for the life cycle of each critical IT System;
- 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 those processing functions;
- Assuming the lead role in resolving Agency security and privacy incidents;
- Abiding by the guidelines established in the Maryland Personal Information Protection Act (PIPA). http://www.oag.state.md.us/idtheft/businessGL.htm

- Development, implementation and testing of an IT Disaster Recovery Plan for critical agency IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users;
- Abiding by the Records Management Guidelines established by the Department of General Services and the Maryland State Archives; http://msa.maryland.gov/msa/intromsa/html/record_mgmt/homepage.html
- Identifying 'business owners' for any new system that are responsible for:
    - Classifying data;
    - 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 State employees and contract personnel are responsible for:

- Being aware of and complying with statewide and internal policies and their responsibilities for protecting IT assets of their agency and the State;
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State or agency; and
- Being accountable for their actions relating to their use of all IT Systems.

SECTION 3: Asset Management

All major information systems assets shall be accounted for and have a named business owner. Accountability for assets helps to ensure that appropriate protection is maintained. Business 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 business owner of the asset.

3.0 Inventory of Assets

Compiling an inventory of assets is an important aspect of risk management. Agencies need to be able to identify their assets and the relative values and importance of these assets. Based on this information, agencies can then provide appropriate levels of protection. Inventories of the important assets associated with each information system should be documented and maintained. Asset inventories shall include; a unique system name, a system/business owner, a security classification and a description of the physical location of the asset. Examples of assets associated with information systems are:

- 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, portable devices, tablets, smartphones, modems), communication equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units), furniture, accommodation; and
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

3.1 Information Classification Policy

This section provides general requirements for data classification. The classification level definitions emphasize common sense steps to be taken to protect confidential information.

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

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.

Confidential information is non-public information that has been deemed **Personally Identifiable Information (PII), Privileged or Sensitive.**

Personally Identifiable Information (PII)
Personally identifiable information is defined as data elements such as an individual's name combined with any one of the following; social security number, driver's license number, financial, tax or health records.

Privileged
Privileged records are 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; and
- 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.

Sensitive
Sensitive is used to define information that, if divulged, could compromise or endanger the citizens or assets of the State.

If an employee is uncertain of the classification of a particular piece of information, the employee should contact their manager for clarification.

All confidential information should be clearly identified as "Confidential" and will be subject to the following handling guidelines.

3.1.1 Guidelines for Marking and Handling State Owned Information

It is necessary to classify information so that every individual that comes in contact with it knows how to properly handle and/or protect it.

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 Policy in the following section*).
- 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 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 identified as "Confidential".
- Access: Only those Maryland State employees or contractors 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.
- Distribution within State of Maryland systems; Delivered direct - signature required, envelopes stamped Confidential, or an approved, 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 encrypted electronic file transmission method.
- Storage: Physically control access to system media (paper and digital) and protect confidential data using encryption technologies and/or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring and strict database change monitoring). Storage is prohibited on portable devices and publicly accessible systems unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on portable devices or publicly accessible systems must be encrypted. 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 storage media is sanitized or destroyed using an approved method. *Refer to Physical Security section of this document.*

Confidential information should be protected with 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. 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 encryption technology. When cryptography is employed within information systems, the system must perform all cryptographic operations using FIPS 140-2 validated cryptographic modules with approved modes of operation. 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.

3.2 System Security Categorization Policy

This section defines common security category levels for information systems that provides a framework that promotes effective management and oversight of information security programs. Formulating and documenting the security level of an information system helps to determine the level of effort or controls required to protect it.

This policy shall apply to all information systems within the State government. Agency officials shall use the security categorizations described in FIPS Publication 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf). Additional security designators may be developed under the framework of FIPS and used at agency discretion.

The security categories are based on potential impact to an agency should certain events occur which jeopardize the information and information systems needed by that agency 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 agency.

Security Objectives
The Federal Information Security Management Act (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 (low, moderate, high) 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 overall State 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. Clarification: 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 agency 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.

Clarification: 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 agency is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to agency 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.

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 agency operations, organizational assets, or individuals. Clarification: 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 agency is not able to perform one or more of its primary functions; (ii) result in major damage to agency 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

3.3 Security Categorization Applied to Information Systems

Determining the security category of an information system requires consideration of the sensitivity of the information resident on that system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be considered at least 'moderate' if the information stored on them is considered 'confidential'. 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.

SECTION 4: Security Control Requirements Overview

This section defines requirements that must be met for agencies to properly protect confidential information under their administrative control. All information systems (hosted on a State network or a 3rd Party offsite premise) used for receiving, processing, storing and transmitting confidential information must be protected in accordance with these requirements. 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) 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*. Only 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 reference NIST SP 800-53 rev.3 for guidance in applying appropriate additional security controls.

This framework categorizes security controls into three types:

1) Management,
2) Operational, and
3) Technical.

Management security controls focus on managing organizational risk and information system security and devising sufficient countermeasures for mitigating risk to acceptable levels. Management security control families include risk management, security assessment and authorization, security planning, and system and services acquisition.

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or a group of systems. Operational security controls require technical or specialized expertise and often rely on management and technical controls. Operational security controls include awareness and training, configuration management, contingency planning, incident response, maintenance, media protection, physical and personnel security, and system and information integrity.

Technical security controls focus on operations executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

SECTION 5 Management Level Controls

5.0 Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for any agency to successfully implement and maintain an acceptable level of security. 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 their systems. Agencies will define a schedule for on-going risk management review and evaluation based on the system categorization level and/or data classification of their systems.

Risk *assessment* is the first process of risk management. Agencies shall use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its System Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. NIST SP 800-30 rev.1 *Guide for Conducting Risk Assessments* provides guidance for carrying out each of the steps in the risk assessment process, such as planning, executing, communicating results, and maintaining the assessment.

Risk *mitigation*, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Controls are defined as IT processes and technologies designed to close vulnerabilities, maintain continuity of operation at specified performance levels, and achieve and document compliance with policy requirements. The controls presented in this section are designed to mitigate risks and are required to comply with this policy.

The third process of risk management, *evaluation*, is ongoing and evolving. Evaluation emphasizes the good practice to develop an effective risk management program within the agency's information 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 SDLC for new systems and applications.

NIST Guidance:

Managing Information Security Risk: Organization, Mission, and Information System View
SP800-39-final.pdf
Information Security Handbook: A Guide for Managers
SP800-100-Mar07-2007.pdf

5.1 Security Assessment and Authorization

Agencies shall produce an Authorization to Operate (ATO) document that verifies security controls have been adequately implemented (or plan to be implemented) to protect confidential information. The ATO constitutes the agency's acknowledgment and acceptance of risk associated with the system.

Custodians of confidential information shall, via the completion of a security authorization form, verify the completeness and propriety of the security controls used to protect it before initiating operations. This shall be done for any infrastructure component or system associated with confidential information. The authorization shall occur every three (3) years or whenever there is a significant change (e.g. major software upgrade, implementation of new hardware, change of hosting services, etc.) to the control structure. A senior agency official shall sign and approve the security authorization.

Agencies shall continuously (at least annually) monitor the security controls within their information systems to ensure that the controls are operating as intended. Agencies shall authorize and document all connections from information systems to other information systems outside of the system boundary through the use of service interface agreements and monitor/control system connections on an ongoing basis. Agencies shall annually 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. Refer to NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment* for guidance in choosing applicable assessment methods.

Agencies are responsible to develop and periodically update a Plan of Action & Milestones (POAM) document 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 annual assessments. A Corrective Action Plan (CAP) will identify activities planned or completed to correct deficiencies identified during the Security Assessment 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

NIST Guidance:
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
sp800-37-rev1-final.pdf
Security Guide for Interconnecting Information Technology Systems
sp800-47.pdf

5.2 Planning

Agency security planning controls include system security plans and system security plan updates. Agencies 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. Agencies must develop, document, and establish a set of rules describing their responsibilities and expected system behavior requirement to system security plan.

NIST Guidance:

Guide for Developing Security Plans for Federal Information Systems
sp800-18-Rev1-final.pdf
Building an Information Technology Security Awareness and Training Program
NIST-SP800-50.pdf

5.3 Service Interface Agreements

With the exception of NetworkMaryland provided connections, external network connections shall be permitted only after all approvals are obtained consistent with this policy and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the untrusted 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. 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 untrusted entities;
- Roles and responsibilities of points-of-contact and cognizant officials for both State and untrusted entities;
- Security measures to be implemented by the untrusted organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection; and
- Requirements for notifying a specified State official within a specified period of time (4 hours recommended) of a security incident on the network.

SECTION 6 Operational Level Controls

6.0 Awareness and Training

Agencies must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to systems. Agencies must identify personnel with information system security roles and responsibilities, document those roles and responsibilities, and provide sufficient security training before authorizing access to information systems or confidential information. Agencies must document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

6.1 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.
- Network devices should be patched and updated for all security related updates/patches using automated tools when possible.
- Develop, document, and maintain 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 provide 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:

Microsoft Security Compliance Manager
http://technet.microsoft.com/en-us/library/cc677002.aspx
National Checklist Program Repository
http://web.nvd.nist.gov/view/ncp/repository
National Security Agency
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
The Center for Internet Security
http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks

6.2 Contingency Planning

Agencies shall develop, implement, and test an IT Disaster Recovery plan for all systems determined to be business critical. Creation, maintenance, and annual testing of a plan will minimize the impact of recovery and loss of information assets caused by events ranging from a single disruption of business to a disaster. Disaster Recovery Plan maintenance should be incorporated into the agency's change management process to ensure plans are up-to-date. Planning and testing provides a foundation for a systematic and orderly resumption of all computing services within an agency when disaster strikes.

Primary Components of an IT Disaster Recovery Plan are;

- Identification of a disaster recovery team;
- Definitions of recovery team member responsibilities;
- Documentation of each critical system including;
    - Purpose
    - Hardware
    - Operating System
    - Application(s)
    - Data
    - Supporting network infrastructure and communications
    - Identity of person responsible for system restoration
- System restoration priority list;
- Description of current system back-up procedures;
- Description of back-up storage location;
- Description of back-up testing procedures (including frequency);
- Identification of disaster recovery site including contact information;
- System Recovery Time Objective RTO;
- System Recovery Point Objective RPO (how current should the data be?); and
- Procedures for system restoration at backup and original agency site.

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

6.3 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. Refer to NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for guidance in creating an incident management policy and developing plans and procedures to support it.

In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout Maryland state government and supported agencies, it is necessary for the agency incident response teams to adopt a common set of terms and relationships between those terms. All elements of state government should use a common taxonomy. A high level set of concepts and descriptions to enable improved communications among and between agencies is provided below. 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. After verifying that an incident has occurred, classify the incident using the categories listed below, follow an incident checklist (See Appendix F) and Report the incident to DoIT.

Agency Incident Categories

Category	Name	Description
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
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.
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.
CAT 4	Improper Usage	A person violates acceptable computing use policies as defined in Section 11 of this document.

Agencies shall report IT incidents to DoIT by completing an IT Incident Report (Appendix A). Agencies are asked to provide as much information about the incident as possible including; the incident category, how the incident was discovered, affected IP addresses, port numbers, information about the affected agency system, impact to the agency, and the final resolution.

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

6.4 Maintenance

Agencies must 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 maintenance on information systems.

Agencies must ensure that system maintenance is scheduled, performed, and documented in accordance with manufacturer or vendor specifications and/or organizational requirements.

6.5 Media Protection

The purpose of this section is to ensure proper precautions are in place to protect confidential information stored on media.

All media that contains confidential information 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.

Media labeled "Confidential" shall be physically controlled and securely stored.

Agencies must protect and control "Confidential" system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Agencies must deploy a tracking method to ensure "Confidential" system media reaches its intended destination.

When no longer required for mission or project completion, media to be used by another person within the agency shall be overwritten (clear or purge) with software and protected consistent with the classification of the data. Specific procedures shall be documented in the applicable agency IT System Security Plan.

Throughout the lifecycle of IT equipment, there are times when an agency will be required to relinquish custody of the asset. The transfer of custody may be temporary, such as when equipment is serviced or loaned, or the transfer may be permanent; examples being a donation, trade-in, lease termination or disposal through GovDeals.com. Any transfer of custody of equipment poses a significant risk that confidential information, licensed software or intellectual property stored on that equipment may also be transferred.

To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*.

Note: Disposal of electronic storage media should be in compliance with the agency's document retention policy and litigation hold procedures.

Several factors should be considered along with the security categorization of the system when making sanitization decisions. Disposal decisions should be made based upon the classification of the data, level of risk, and cost to the agency. DoIT endorses two options for sanitization:

Option 1: If the storage device in a unit designated for re-sale or disposal is over four years old, it must be destroyed.

Option 2: If the storage device in a unit designated for re-sale or disposal is less than four years old, it must be sanitized with a disk wiping utility such as Active Killdisk Professional or destroyed.

Additionally, the procedures performed to sanitize electronic media should be documented and retained for audit verification purposes.

This policy applies to all electronic storage media equipment that is owned or leased by the State (including, but not limited to: workstations, servers, laptops, cell phones and Multi-Function Printers/Copiers).

For situations in which the electronic storage media leaves the custody of the agency temporarily, such as servicing of equipment or a temporary loan of equipment outside of an agency, the agency 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 agency shall remove the hard drive. If removal of the hard drive is not feasible, the agency shall sanitize the equipment or encrypt the information commensurate with the assessment of the information contained on the hard disk.

Agencies can outsource media sanitization and destruction if business and security management decide that this would be the most reasonable option for them to maintain confidentiality while optimizing available resources. When exercising this option, this guide recommends that organizations exercise “due diligence” when entering into a contract with another party engaged in media sanitization.

Due diligence could include;

- 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.

Note on solid state drives; A solid-state drive (SSD) is a data storage device that uses solid-state memory to store persistent data. Standard sanitation methods have proven ineffective for SSD's. State sanitation standards for SSD's containing confidential information require:

- Physical destruction, or
- Encrypt the entire disk as soon as the operating system is installed.

6.6 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. Agencies must:

- Secure IT areas with controls commensurate to the risks;
- Ensure secure storage of media; and
- 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;
- Power and emergency backup equipment; and
- Operations and control areas.

Access to data centers and secured areas should be limited to those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be:

- Based on frequency of need for access; and
- Approved by the manager responsible for the secured area.

Each agency 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;
- Ensuring proper employee/contractor identification processes are in place;
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems; and
- Ensuring that any physical access controls are auditable.

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.

6.7 System and Information Integrity

Agencies shall implement system and information integrity security controls including flaw remediation, information system monitoring, information input restrictions (such as validating input in all Web applications), and information output handling and retention.

Agencies must protect against malicious code (e. g. viruses, worms, Trojan horses, etc.) by implementing (anti-virus, anti-malware) solutions that, to the extent possible, includes a capability for automatic updates. Intrusion detection/prevention tools and techniques

must be employed to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

Agencies 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.

Agencies must identify, document, and correct information system flaws.

Agencies shall receive and review information system security alerts/advisories for critical software that they use (e. g. operating systems, applications, etc.) on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

Agencies 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

7.0 Access Control Requirements

- Agencies must manage user accounts, including activation, deactivation, changes and audits.
- Agency systems must enforce assigned authorizations that control system access and the flow of information within the system and between interconnected systems.
- Agencies must 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".
- Agencies must 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.
- Agencies must ensure that the systems enforce separation of duties through assigned access authorizations. Agency systems must enforce the most restrictive access capabilities required for specified tasks.
- Agency systems must 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.
- Agency systems must display the following warning before granting system access;
  "Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or 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 this system are the property of State of Maryland and may be used by the State of Maryland for any purpose."

- Agency systems must 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.
- Agencies must 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.
- Agencies must develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required). 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 maintaining external information systems, allowing authorized individuals to; (i) access the information system from the external information systems; and (ii) process, store, and/or transmit agency-controlled information using the external information systems.
- Agencies must authorize, document, and monitor all wireless access to its information systems. Wireless security guidelines are documented in Appendix D.
- Devices which are not the property of, or under the control of an Agency (including any portable devices) should not be directly attached to the Agency networks.

7.1 Audit & Accountability Control Requirements

- Information systems must generate audit records for all security-relevant events, including all security and system administrator accesses. An example of an audit activity is reviewing the administrator actions whenever security or system controls may be modified to ensure that all actions are authorized. 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 be enabled for 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 an application. The information system shall be configured to alert appropriate agency officials in the

event of an audit processing failure and take the additional actions (i.e. shut down information system, overwrite oldest audit records or stop generating audit records).

- Information systems must be configured to allocate sufficient audit record storage capacity to record all necessary auditable items. Refer to NIST SP 800-92 *Guide to Computer Security Log Management* (table 4.1) for guidance on local system log retention configuration options. Agencies shall ensure that its information systems produce audit records that contain sufficient information to, at a minimum establish; (i) what type of event occurred, (ii) when (date and time) the event occurred, (iii) where the event occurred, (iv) the source of the event, (v) the identity of the targeted resource (vi) the outcome (success or failure) of the event, (vii) the identity of any user/subject associated with the event.
- Procedures must be developed to routinely (for example 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, Agencies must ensure that audit information is archived for the [lesser of 3 years or until the Office of Legislative Audits completes the audit of the entity] to enable the re-creation 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.

7.2 Identification & Authorization Control Requirements

- 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.
- Agencies must manage user accounts assigned within its information systems. Effective user account management practices include (i) obtaining authorization from appropriate officials to issue user accounts to intended individuals; (ii) disabling user accounts, when no longer needed. (immediately upon user exit from employment, 60 days for inactive accounts.); (iii) not re-issuing 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.
- 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.

7.2.1 User Authentication & Password Requirements

All users must be uniquely identified. 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;
- Change user-level passwords at regular intervals (at least annually);
- Administrative-level account passwords shall be changed every 90 days or sooner;
- Passwords protecting access to systems or applications that have been categorized as Moderate or High shall be changed every 90 days or sooner;
- 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);
- State issued login credentials (username & password) shall not be used for ancillary 3rd party services (online Web accounts, e-mail, e-commerce, etc..)
- A password 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 fifteen (15) minute automatic reset of the account;
- User ids associated with a password must be disabled or locked after 60 days of inactivity; and
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

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., RACF ID used to run production jobs). Passwords associated with functional IDs must not be stored in clear text, must have a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters, and must not be displayed on the screen. Functional IDs are exempt from the other user password characteristics described above.

7.3 System & Communications Control Requirements

- 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 confidential information during electronic transmission. Agencies must encrypt all media containing confidential information during transmission. 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.
- 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. Exceptions can be authorized in writing by the agency CIO or authorizing official.

SECTION 8 Virtualization Technologies

Agencies must implement careful planning prior to the installation, configuration and deployment of virtualization solutions to ensure that the virtual environment is as secure as a non-virtualized environment and in compliance with all relevant state and/or agency policies. Security should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize costs. The security recommendations described 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

Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. If an agency plans on using a cloud-based solution for processing, transmitting or storing confidential information, security controls must be implemented to ensure that the compliance and

auditing requirements are met as stated in this policy in addition to any Federal regulations that may apply.

NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing* provides an overview of the security and privacy challenges for public cloud computing and present recommendations that agencies should consider when outsourcing data, applications and infrastructure to a public cloud environment. Maryland shall adopt the security recommendations and guidelines described in SP 800-144. The key guidelines recommended to agencies include:

Preliminary Activities;

- Identify security, privacy, and other organizational requirements for cloud services to meet, as a criterion for selecting a cloud provider.
- Analyze the security and privacy controls of a cloud provider's environment and assess the level of risk involved with respect to the control objectives of the organization. A review of the provider's SOC 2 report is helpful.
- Evaluate the cloud provider's ability and commitment to deliver cloud services over the target timeframe and meet the security and privacy levels stipulated.

Initiating and Coincident Activities;

- Ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider.
- Involve a legal advisor in the review of the service agreement and in any negotiations about the terms of service.
- Continually assess the performance of the cloud provider and the quality of the services provisioned to ensure all contract obligations are being met and to manage and mitigate risk.

Concluding Activities;

- Alert the cloud provider about any contractual requirements that must be observed upon termination.
- Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner.
- Ensure that organizational resources made available to or held by the cloud provider under the terms of service agreement are returned or recovered in a usable form, and that information has been properly expunged.

Guidelines on Security and Privacy in Public Cloud Computing
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494
Cloud Computing Synopsis and Recommendations
http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

SECTION 10: Mobile Devices

Tablets, and other mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain. Laptops are specifically excluded from the scope of this policy because the security controls available for laptops today are quite different than those available for mobile devices.

The most effective way to secure confidential data is not to store it on mobile devices. As a matter of policy and best practice, data should always be secured where it resides.

State business requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, Agencies are required to assure that steps have been taken to keep the data secure. It is the responsibility of the agencies to recognize these risks and take the necessary steps to protect and secure their mobile computing devices. Consideration of a mobile device management solution may be necessary to implement recommended controls.

Steps may include, but are not limited to:

- A list of supported mobile devices.
- Protection of data transmission that occurs between the mobile device and the agency assets.
- Protection of data storage on mobile devices including removable media.
- Procedures that should be followed if a mobile device is lost or is at risk of having its data recovered by an untrusted party (proper authority notification and device wipe options).
- All vendor recommended patches, hot-fixes or service packs must be installed prior to deployment and processes must be in place to keep system hardware, operating system and applications current based on vendor support recommendations (including patches, hot-fixes, and service packs);
- Proper asset management procedures shall apply to all mobile devices;
- Whenever possible, all mobile device application distribution and installation shall be centrally controlled and managed;
- Whenever possible, all mobile device operating system and application security patch installation shall be centrally controlled and managed;
- Mobile device options and applications that are not in use shall be disabled;
- Whenever possible, Bluetooth settings should be configured to notify users of incoming connection requests and to receive confirmation before proceeding;
- All mobile devices must be password or PIN protected;
- All mobile devices should have timeout/locking features and device erase functions (including removable memory) enabled;
- Whenever possible, all mobile devices should have anti-virus and/or firewall protection installed;

- No confidential information shall be stored on mobile devices unless it is encrypted and permission is granted from an authorized official;
- Confidential information should be sanitized from the mobile device before it is returned, exchanged or disposed of; and
- Whenever possible, mobile devices shall be scanned for viruses/malware before they can connect to State systems;

The physical security of State issued mobile devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight. If a mobile device is lost or stolen, the employee is responsible for promptly reporting the incident to the proper authorities and all business applications shall be wiped.

NIST Guidance:
Guidelines for Managing and Securing Mobile Devices in the Enterprise
http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

SECTION 11: 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.

This document sets forth policy of the State 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 Executive Departments and Independent State Agencies. The purpose of this policy is to explain the ownership of the electronic communications created, received, or stored on the State electronic communications systems and to inform users of the systems about their rights and duties with respect to electronic communications.

This section applies to users of State electronic communications systems and may be changed by the Agency, in its discretion, without prior notice. This policy is in addition to, and not in replacement of, any other published policy or code of conduct of Executive Departments and Independent State Agencies.

Any non-government business use or intentional misuse of the State's electronic communications systems is a violation of this policy. Non-government business uses include, but are not limited to:

- Sending and responding to lengthy private messages;
- Sending political messages; and

- Operating a business for personal financial gain.

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 without a government business purpose. It also includes attempting to access a secure database, whether private or public, without permission.

The State's electronic communications systems may be used for minor, incidental personal uses, as determined by 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.

Users shall have no expectation as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses. 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.

The State reserves the right to monitor compliance with this policy by accessing, intercepting, recording, or disclosing any electronic communications , including minor incidental personal uses, unless prohibited by law or privilege.

The State reserves the right to access, intercept, inspect, record, and disclose any electronic communications 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 the Executive Departments or Independent State Agencies or disclosure is necessary to support the business of the government.

Users are not permitted to hinder or obstruct any security measures instituted on the State's electronic communication systems.

11.0 Acceptable/Proper Use

The following activities are examples of acceptable use of agency electronic communications:

- Sending and receiving electronic mail for job related messages, including reports, spreadsheets, maps etc.
- Using electronic mailing lists and file transfers to expedite official communications within and among state agencies, as well as other job related entities.
- Accessing 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.
- Connecting with other computer systems to execute job related computer applications, as well as exchange and access datasets.
- Communicating with vendors to resolve technical problems.

11.1 Unacceptable/Improper Use

The following activities are examples of 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.
- Unauthorized collection, transmission or sharing of Confidential information which may include; Personally Identifiable Information, HIPPA protected information and Federal Tax Information ;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 DoIT.

- 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.

User's access to State electronic communications systems resources shall cease 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;
- End of public official's term; or
- Lay-off of employee.

SECTION 12: Social Media Policy

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 department or agency, considering its mission, objectives, capabilities, and potential benefits.

The purpose of this section is to provide rules of conduct to State organizations and State employees when using social media technologies to engage with citizens on behalf of the State of Maryland. The State expects all authorized participants in social media on behalf of the State to understand and to follow these guidelines.

Should an agency choose to use social media networks, the agency should sanction official participation and representation on specific social media sites. State agencies have 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. Furthermore, any non-government business use or intentional misuse of social media communications systems is a violation of this policy. Misuse of social media and prohibited activities include, but are not limited to:

- Sending and responding to private messages that are not related to state business;
- Engaging in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups;

- Endorsement of commercial products, services, or entities;
- Endorsement of political parties, candidates, or groups;
- Lobbying; and
- Posting photos or videos that are not related to the mission of the agency.

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.

12.0 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 State 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 necessarily represent Maryland's positions, strategies or opinions."
- Organizational, originating from a State Organization controlled social media site: The State Organization must disclose the following information as part of their use of a communication channel: Organization 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).

12.1 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.

12.2 Ethical Conduct

State employees and organizations will act and conduct themselves according to the highest possible ethical standards. A summary of the key points of ethical social media conduct are reproduced below:

- Should an agency choose to use social media networks, state employees shall be familiar with and comply with the terms and conditions of the social media site.
- State employees and State organizations 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. Agencies will strive to correct any information found to be in error.
- State employees and State organizations must maintain confidentiality of State of Maryland information that is considered to be confidential in nature.
- State employees and State organizations will respect the rules of the Social Media venue.

12.3 Guiding Principles

If you are developing a social media site on behalf of the state, utilize the state guidance provided at: http://blogs.maryland.gov/socialmedia/

If you participate in social media, it is recommended that you adhere to these guiding principles:

- 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
- Agencies should consider posting a disclaimer stating that information within the social media site is public information and the state cannot be responsible for blocking such access.

12.4 Secure Practices

- 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 unauthorized users 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.
- Security technologies shall be implemented to protect State-represented social media sites from unwanted user-generated content.

SECTION 13: Data Loss Prevention Guidance

If currently implemented security controls have failed to reduce agency information security risk to an acceptable level, a data loss prevention solution should be considered.

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use, data in motion, and data at rest, through deep content inspection and with a centralized management framework. DLP solutions go beyond securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. A comprehensive DLP solution should include the following controls.

- Use network monitoring tools to analyze outbound traffic looking for anomalies which may include; large file transfers, long-time persistent connections, connections at regular repeated intervals, unusual protocols and ports in use, and possibly the presence of certain keywords in the data traversing the network perimeter;
- Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel;
- The ability to scan systems using automated tools to determine whether confidential data is present in clear text;
- Use outbound proxies to be able to monitor and control all information leaving an organization;
- Use secure, authenticated, and encrypted mechanisms to move data between untrusted networks;
- Data stored on removable and easily transported storage media such as USB tokens (i.e., "thumb drives"), USB portable hard drives, and CDs/DVDs should be encrypted. Systems should be configured so that all data written to such media are automatically encrypted without user intervention;
- If there is no business need for supporting such devices, organizations should configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data

placed on such devices. An inventory of all authorized devices must be maintained;

- Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.
- DLP solutions should be tested periodically with results documented. Results of the tests can help identify if a business or technical process is leaving behind or otherwise leaking confidential information.

CSIS: 20 Critical Security Controls - Version 3.1
http://www.sans.org/critical-security-controls/control/17

SECTION 14 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. 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.

Appendix A: IT Incident Reporting Form

IT Incident Reporting Form

Agency;_____

Date and time of Incident;_____

Point of Contact Name;_____Phone;

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

Incident Category;

1 Unauthorized access
2 Denial of Service
3 Malicious Code
4 Improper Usage

Incident discovery method;

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 describe the incident including the impact to your agency;

What actions were taken to reduce the risk of this type of incident happening again?

Does your agency require any additional assistance from DoIT?

Appendix B: Definitions

Approved Electronic File Transmission Methods	Includes Virtual Private Network (VPN) tunnels supported by Executive Departments and Independent State Agencies.
Approved Electronic Mail	Includes all mail systems supported by Executive Departments and Independent State Agencies.
Confidential Information	Non-public information that is deemed private, privileged or sensitive.
Critical Information	System-level security settings or configurations.
Electronic Communications	Including, but not limited to, messages, transmissions, records, files, data, and software, whether in electronic form or hardcopy.
Electronic Communications 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 knowledge, usually referred to as a key.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.
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 Device	Devices such as smart phones and tablets that can connect to networks.
Network	A computer network is a system for communication among two or more computers.
Network Device	Includes; servers, desktop computers, laptop computers, printers, scanners, photocopiers, personal computing devices and other computing devices with networking interfaces capable of connecting to the Agency's network.
Obfuscation	To make obscure; using methods to hide the actual values of sensitive data.
Private	Personally Identifiable Information (PII); such as an individual's social security number, financial or health records.
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.
Portable Device	Any electronic portable device capable of storing data such as; Laptops, Mobile or Smart phones, MP3 Players, USB Thumbdrives, External Hard Drives, iPads, etc.

Publicly Accessible System	Systems such as Web and FTP applications that are exposed to the Internet and therefore, more vulnerable.
Public Information	Information that is a public record under the Maryland Public Information Act.
Remote Access	Any access to DoIT's managed network through a non-DoIT managed network, device, or medium.
Sanitization	Refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.
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.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Untrusted Entity	An entity that can or may be potentially harmful to a system.
Wi-Fi Certified	Wi-Fi CERTIFIED is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability

Appendix C: Wireless Security

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to any state agency network. 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. Agencies shall;

- Establish a process for documenting all wireless access points;
- Ensure proper security mechanisms are in place to prevent the theft, alteration, or misuse of access points;
- Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available;
- Change default administrator credentials;
- Change default SNMP strings if used, otherwise disable SNMP;
- Change default SSID;
- Deploy secure access point management protocols and disable telnet;
- Strategically place and configure access points to minimize SSID broadcast exposure beyond the physical perimeter of the building;
- Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services;
- Require wireless users to utilize encrypted data transmission if accessing internal LAN services;

Appendix D: Sample Media Sanitization Form

Organization:
Item Description:
Item Disposition:

- Sanitize
- Destroy

Date Conducted:
Conducted By:
Phone #:
Validated By:
Phone #:
Sanitization Method Used:

Appendix E: Sample Incident Handling Checklist and Forensics Guidelines

Action	Done
Detection and Analysis	
Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
Identify which resources have been affected and forecast which resources will be affected	
Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery	
Acquire, preserve, secure, and document evidence	
Contain the incident	
Eradicate the incident	
Identify and mitigate all vulnerabilities that were exploited	
Remove malicious code, inappropriate materials, and other components	
Recover from the incident	
Return affected systems to an operationally ready state	
Confirm that the affected systems are functioning normally	
If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity	
Create a follow-up report	
Hold a lessons learned meeting	

Refer to the corresponding tables within NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for specific incident category guidance.
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Incident Response and Forensics Guidelines

Preserving forensic data is an essential aspect of any incident response plan. The forensic data acquired during the overall incident response process is critical to containing the current intrusion and improving security to defend against a similar future attack. The following guidelines are provided to assist agencies in the retention of essential forensic data.

Keep detailed notes of all observations, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.

When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.

Capture a forensic image of the system memory prior to powering down the system.

When powering down a system, physically pull the plug from the wall rather than gracefully shutting down. Forensic data can be destroyed if the operating system (OS) executes a normal shut down process.

After shutting down, capture forensic images of the host hard drives.

Avoid running any antivirus software "after the fact" as the antivirus scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.

Avoid making any changes to the OS or hardware, including updates and patches, as they might overwrite important information relevant to the analysis. Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts.

When a compromised host is identified, it should be removed from the network for forensic data collection (but not powered off, as noted above). When all available data have been retained from the infected host, agencies should follow established internal procedures for recovering the host.

If an agency does not have an adequate incident response plan or the necessary staff to handle a serious cyber incident, it should consult trained forensic investigators to assist with developing a response plan and implementing recovery efforts.

Useful imaging tool by Access Data (FTK Imager) can be used to capture and preserve evidence.
http://www.accessdata.com/support/product-downloads