



DEPARTMENT OF INFORMATION TECHNOLOGY
INFORMATION SECURITY POLICY

Version 2.2

October 2009

TABLE OF CONTENTS

PURPOSE	3
SCOPE	3
AUTHORITY	3
RECORD OF REVISIONS	3
SECTION 1: PREFACE	3
SECTION 2: ROLES AND RESPONSIBILITIES	4
2.0 DEPARTMENT OF INFORMATION TECHNOLOGY	4
2.1 AGENCY	4
2.2 EMPLOYEES AND CONTRACTORS	5
SECTION 3: ASSET MANAGEMENT	5
3.0 INVENTORY OF ASSETS	5
3.1 INFORMATION CLASSIFICATION POLICY.....	5
3.2 SYSTEM SECURITY CATEGORIZATION POLICY	7
3.3 SECURITY CATEGORIZATION APPLIED TO INFORMATION SYSTEMS	8
SECTION 4: SECURITY PROGRAM	9
4.0 IT SECURITY POLICY.....	9
4.1 RISK MANAGEMENT.....	10
4.2 SYSTEMS DEVELOPMENT LIFE CYCLE METHODOLOGY	10
4.3 SYSTEM CERTIFICATION AND ACCREDITATION.....	11
4.4 IT DISASTER RECOVERY PLAN	12
4.5 SECURITY AWARENESS	12
4.6 IT INCIDENT RESPONSE PROCESS.....	13
SECTION 5: ELECTRONIC COMMUNICATIONS	13
5.0 ACCEPTABLE USE	15
5.1 UNACCEPTABLE USE.....	15
SECTION 6: PHYSICAL SECURITY	16
6.0 SECURED IT AREAS	16
6.1 STORAGE AND MARKING	16
6.2 PERSONNEL	16
6.3 STORAGE MEDIA REUSE	17
6.4 STORAGE MEDIA DISPOSAL	17
SECTION 7: NETWORK SECURITY	17
7.0 LOCAL NETWORK ACCESS	18
7.1 DIAL-IN ACCESS.....	18
7.2 BANNER TEXT POLICY	18
7.3 FIREWALLS & NETWORK DEVICES.....	19
7.4 INTRUSION DETECTION POLICY.....	19
7.5 SERVICE INTERFACE AGREEMENTS.....	20
7.6 REMOTE ACCESS.....	20
7.7 ACTIVE CONTENT	20

7.8	WIRELESS	21
7.9	PRIVATE BRANCH EXCHANGE (PBX)	22
SECTION 8: ACCESS CONTROL		22
8.0	AUTHENTICATION	22
8.1	PASSWORD CONSTRUCTION RULES AND CHANGE REQUIREMENTS	23
8.2	AUTHORIZATION	23
8.3	AUDIT TRAIL.....	23
8.4	VIOLATION LOG MANAGEMENT AND REVIEW	24
SECTION 9: COMMUNICATION AND OPERATIONS MANAGEMENT		24
SECTION 10: POLICY VIOLATIONS		26
APPENDICES		27
	APPENDIX A: COMPUTER SECURITY INCIDENT HANDLING FORM.....	28
	APPENDIX B: DEFINITIONS	29

PURPOSE

The purpose of this Policy is to describe a set of minimum 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 best practice for all other State agencies. Any agency may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), exceed the security requirements expressed in this document, but must, at a minimum, conform to the security levels required by this Policy.

SCOPE

This policy applies to all information that is electronically generated, received, stored, printed, filmed, and typed. The provisions of this policy apply to all units in the Executive Branch of the State of Maryland 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.

SECTION 1: Preface

Information and 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 information from unauthorized access, modification, disclosure and destruction. This Policy sets forth a minimum level of security precautions that, when implemented, will protect the confidentiality, integrity and authentication of IT assets.

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;
- 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 also responsible for:

- Implementing and maintaining an Agency IT Security Program
- Monitoring and enforcing the IT Security Program within their agency;
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency security program;
- Managing the Agency Security Program and initiating measures to assure and demonstrate compliance with security requirements;
- Ensuring that security is part of the information planning and procurement process;
- Implementing an IT Security Certification and Accreditation process for the life cycle of each agency critical IT System;
- Identifying security vulnerabilities within Agency systems and recommending corrective action;
- Assessing the adequacy and coordinating the implementation of specific information security controls for new systems or services;
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions;
- Assuming the lead role in resolving Agency security and privacy incidents;
- Documenting and ensuring that a process is implemented for the classification of information in accordance with the Policy for Classifying Confidential Information;
- Specifying the level of security required to protect all information assets under their control to comply with this Policy;
- Ensuring a configuration/change management process is used to maintain the security of the IT system;
- Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems in accordance with IT Disaster Recovery Plan Guidelines;
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users.

Each state agency shall identify system 'data owners' (usually business unit managers) that are responsible for:

- Classifying data;
- Approving access and permissions to the 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 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 owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners shall be identified for all major assets and the responsibility for the maintenance of appropriate controls shall be assigned. Responsibility for implementing controls may be delegated. Accountability shall remain with the named owner of the asset.

3.0 Inventory of assets

Inventories of assets help ensure that effective asset protection takes place. 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 levels of protection commensurate with the value and importance of their assets. Inventories of the important assets associated with each information system should be drawn up and maintained. Each asset should be clearly identified and its ownership and security classification agreed and documented, together with its current location (important when attempting to recover from loss or damage). 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, modems), communications equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units), furniture, accommodation;
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning.

3.1 Information Classification Policy

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

All confidential information should be clearly marked “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 high negative impact to the State of Maryland, its’ employees or citizens and may include information or records deemed as Private, Privileged or Sensitive.

- Marking: Confidential information is to be clearly marked as “Confidential”.
- Access: Only those Maryland State employees with explicit need-to-know and other individuals for whom an authorized Maryland State official has determined there is a mission-essential need-to-share and the individual has signed a non-disclosure agreement.
- Distribution within State of Maryland systems; Delivered direct - signature required, envelopes stamped Confidential, or an approved, encrypted electronic email or electronic file transmission method.
- Distribution outside of State of Maryland systems: Delivered direct; signature required; approved private carriers; or approved encrypted electronic email or electronic file transmission method.
- Storage: Physically control access to and securely store information system media, both paper and digital, based on the highest security category of the information recorded on the media. Storage is prohibited on portable devices unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on portable devices must be encrypted. Refer to State IT Security Policy and Standard State Data Encryption Standard. Keep from view by unauthorized

individuals; protect against viewing while in use and when unattended, store in locked desks, cabinets, or offices within a physically secured building.

- Disposal/Destruction: Dispose of paper information in specially marked disposal bins on Maryland State premises or shred; electronic media is sanitized or destroyed using an approved method. *Refer to Physical Security section of this document.*

Confidential information is prohibited on portable devices and non-state owned devices unless prior written approval from agency Secretary (or delegated authority) has been granted. Approved storage on any portable or remote access device must be encrypted. 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 policy defines common security category levels for information systems providing 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 required for security certification and accreditation.

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 FIOS and used at agency discretion.

The security categories are based on potential impact on 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, medium, 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 organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is **MODERATE** if—

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

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 the highest 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**.

It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate worst case potential impact for the overall information system—thereby averting the need to consider the system processes in the security categorization of the information system.

SECTION 4: Security Program

An effective enterprise-wide information security program provides a strong foundation for understanding and implementing security throughout an agency. This Policy identifies key components that must be considered by an agency when implementing, reviewing, or seeking to improve the value of its information security program. It is encouraged that these components be reviewed for applicability to an agency's business environment and compliance with existing laws and policies, and implemented as appropriate for each agency. Some agencies may not require all components, but where a component is applicable to an agency's program, it should be adopted and implemented. Each agency is responsible for developing an IT Security Program illustrating how it will protect the agency's IT infrastructure in accordance with this State IT Security Policy. The following are minimum components that must be included within the program:

- IT Security Policy
- Risk Management Process
- Systems Development Life Cycle Methodology
- IT Security Certification and Accreditation
- IT Disaster Recovery Plan
- Security Awareness
- IT Incident Response Process

4.0 IT Security Policy

Information security policy is an essential component of information security governance—without the policy, governance has no substance and rules to enforce. Security Policy Management refers to the practices and methods used to create and maintain security policies to translate, clarify, and communicate management's position on high-level security principles. Policy management includes development, deployment, communication, updating, and enforcement of agency security policies.

Agency information security policies should address the fundamentals of agency information security governance structure, including:

- Information security roles and responsibilities.
- Statement of security controls baseline and rules for exceeding the baseline.
- Rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance.

Supporting guidance and procedures on how to effectively implement specific controls across the enterprise should be developed to augment an agency's security policy. This subsequent guidance on information security, created by the agency, in consideration of external guidance (e.g. NIST Special Publications and FIPS), should be consistent with the information security policy and may not supersede it, unless the policy itself is being modified. Agencies should ensure that their information security policy is sufficiently current to accommodate the information security environment and agency mission and operational requirements. To ensure that information security does not become obsolete, agencies should implement a policy review and revision cycle. As a part of the periodic review and the initial development of the information security policies, agencies should work to ensure that all internal security policies (i.e., physical and personnel) are sufficiently coordinated to ensure effective implementation of crosscutting and convergent security objectives, such as access control initiatives.

Important Resources

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

Federal Information Security Management Act (FISMA) Implementation Project

4.1 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 process must be implemented to assess the acceptable risk to agency IT systems as part of a risk-based approach used to determine adequate security for the system. Agencies shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Agencies will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system. Refer to NIST Special Publication 800-30, Risk Management Guide for IT for guidance: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. 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 successful risk management program is a proactive, ongoing process of identifying and assessing risk, and weighing business tradeoffs on acceptable levels of risk against ever changing technologies and solutions.

Risk *assessment* is the first process in risk management. Agencies should use risk assessment to determine the extent of the potential threat and the risk associated with an IT system or an operational function. Depending upon the complexity and criticality of an agency's business, the risk assessment process may encompass up to nine primary steps, which include identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

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 external and internal policy requirements.

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 System Development Life Cycle (SDLC) for new systems and applications.

Important Resources

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

NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers

4.2 Systems Development Life Cycle Methodology

Agencies should ensure that security is an integral part of information systems, which include operating systems, infrastructure, applications and off-the-shelf products, services, and user-developed applications. Security requirements shall be identified and agreed upon prior to the development and/or implementation of information systems and documented as part of the overall business case. The requirements must also ensure compliance with any applicable laws, regulations, statutes, or state policies (e.g., HIPAA, PCI Standards, etc.). Security should be considered and designed in from the beginning and during the entire system development lifecycle. The following are minimum requirements that shall be included as part of the SDLC methodology;

- Implement requirements for ensuring authenticity and protecting message integrity in applications.
- Implement the use of encryption (cryptographic) measures to protect confidential or sensitive information and protect encryption keys from modification, loss and destruction.
- Implement input and output data validation checks to ensure data is correct and appropriate.

- Implement processes to control the installation of software on operating systems.
- Implement procedures to select, protect, and control test data. Do not use test data in a production environment or use production data in a test environment without careful consideration.
- Limit access to program source code and place source code in a secure environment.
- Implement change control procedures to minimize the corruption of information systems.
- Limit modifications to vendor-supplied software packages.
- When outsourcing software development, consider contractual language for licensing arrangements, code ownership, quality and security functionality, testing to detect malicious code, and escrow arrangements in the event of third party failure.

Important Resources

<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html>

U. S. Department of Homeland Security – Build Security In Home

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

NIST SP 800-55 Security Metrics Guide for IT Systems

NIST SP 800-44 Guidelines for Securing Public Web Servers

<http://www.sans.org/top25errors/>

CWE/SANS TOP 25 Most Dangerous Programming Errors

4.3 System Certification and Accreditation

Security *accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. The senior agency official should have the authority to oversee the budget and business operations of the information system. Security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans. Risk assessments can be accomplished in a variety of ways depending on the specific needs of the agency. Some agencies may choose to assess risk informally. Other agencies may choose to employ a more formal and structured approach. In either case, the assessment of risk is a process that should be incorporated into the system development life cycle. At a minimum, documentation should be produced that describes the process employed and the results obtained. System security plans provide an overview of the information security requirements and describe the security controls in place or planned for meeting those requirements. System security plans can include as references or attachments, other important security-related documents (e.g., risk assessments, contingency plans, incident response plans, security awareness and training plans, information system rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, system interconnection agreements) produced as part of an agency's information security program.

In addition to risk assessments and system security plans, security assessments play an important role in security accreditation. It is essential that agency officials have the most complete, accurate and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security *certification* is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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 the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

By accrediting an information system, an agency official accepts the risks associated with operating the system and the associated implications on agency operations, agency assets, or individuals. Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

Important Resources;

http://doit.maryland.gov/support/Documents/security_guidelines/it_security_ca_overview.pdf Introduction to the State of Maryland IT Security Certification and Accreditation Guidelines

http://doit.maryland.gov/support/Documents/security_guidelines/it_security_ca_guidelines.pdf State of Maryland IT Security Certification and Accreditation Guidelines

4.4 IT Disaster Recovery Plan

Agencies shall develop, implement, and test an IT Disaster Recovery plan for each critical system to ensure that contingency procedures will be available in the event of a disaster resulting in the loss of services from the primary production system. 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. Planning and testing provides a foundation for a systematic and orderly resumption of all computing services within an agency when disaster strikes.

Important Resources;

<http://doit.maryland.gov/support/Pages/SecurityDisasterRecovery.aspx>

4.5 Security Awareness

A key component to assure that users understand their role and responsibility for information security is through an ongoing awareness program. Awareness is not training. The purpose of awareness is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. An effective program ensures employees and contractors know about information security and privacy relative to their job responsibilities. A good awareness program promotes the agency's existing policies, standards, and practices.

A successful security awareness program should target various groups (such as employees and contractors, IT staff, or managers and supervisors) with information pertinent to their respective roles. Most users would be interested in awareness material addressing Internet use, email, and handling confidential information.

Technical support personnel would be more focused on access control, anti-virus, and patch management administration. The executives would be more interested in the benefits of enabling business through information security, risk management, and business continuity.

Agencies shall develop and implement a security awareness program that, at a minimum, includes the following;

- Promote security awareness using techniques such as: posters, email messages, formal instruction, web-based instruction, videos, newsletters, and security awareness days.
- Ensure all users sign confidential and acceptable use statements.
- Ensure all users can quickly identify threats, and know how to respond to security incidents.
- Inform all users about agency policies and procedures.
- Regularly review and update training content to reflect changes to the agency's environment.

Important Resources

<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

Building an IT Security Awareness and Training Program

<http://doit.maryland.gov/support/Pages/SecurityAwareness.aspx>

DoIT Security Awareness Web Page

4.6 IT Incident Response Process

Information Security Critical Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. A critical incident is one that can shut down business, disrupt operations, cause physical damage, or that can threaten the agency's financial or public image. Examples of critical incidents could include activity such as:

- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Development, documentation, and implementation of an information security incident response plan provide the framework for an agency to proactively manage incidents when they occur. Agencies shall be required to detect, track, log and report critical security incidents. The speed with which an agency can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. The term damage means "impairment to the integrity or availability of data, a program, a system or information". Agencies should report critical incidents to the DoIT Service Desk (410) 260-7778 or ServiceDesk@doIT.state.md.us. Appendix A contains the Computer Security Critical Incident Handling Form.

SECTION 5: Electronic Communications

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 policy 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.

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.

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,
- Operating a business for personal financial gain, and
- Purchasing goods or services for private uses.

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.

5.0 Acceptable Use

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

- Send and received electronic mail for job related messages, including reports, spreadsheets, maps etc.
- Use electronic mailing lists and file transfers to expedite official communications within and among state agencies, as well as other job related entities.
- Access on line information sources to gather information and knowledge on state and federal legislation, industry best practices, or to obtain specialized information useful to state agencies.
- Connect with other computer systems to execute job related computer applications, as well as exchange and access datasets.
- Communicate with vendors to resolve technical problems.

5.1 Unacceptable 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.
- 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.
- Lay-off of employee.

SECTION 6: Physical Security

Physical access to IT information processing, storage areas, and storage devices and its 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;
- Obtain personnel security clearances where appropriate;
- Ensure secure media reuse;
- Ensure the secure destruction of storage media.

6.0 Secured IT Areas

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;
- Operations and control areas.

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

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

Each agency is responsible for:

- Issuing picture identification badges to all Employees/contractors and ensuring that these badges are openly displayed at all times;
- 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 environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems;
- Ensuring that any physical access controls are auditable.

6.1 Storage and Marking

IT Systems and electronic media shall be protected and marked in accordance with the data sensitivity (see Section 3). Users shall not store data on electronic media that cannot be adequately secured against unauthorized access. Data to be electronically transferred to a remote storage location should be transferred only by a secure and encrypted method.

6.2 Personnel

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.

6.3 Storage Media Reuse

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

6.4 Storage Media Disposal

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 the Department of General Services. Any transfer of custody of equipment poses a significant risk that sensitive information, licensed software and intellectual property stored on that equipment may also be transferred. Despite the application of media clearing processes, in many cases, information that appears to have been removed may be easily recoverable.

This policy applies to all electronic storage media equipment that is owned or leased by the State. This may also include cell phones. The purpose of this policy is to ensure secure handling of electronic storage media containing State data, licensed software, and intellectual property at the time of disposal, servicing or transfer of State agency IT equipment.

To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will physically remove all hard drives when permanently relinquishing custody of IT equipment. The removed hard drives may either be re-used within an agency or must be physically destroyed such that they are permanently rendered functionally useless. Agency CIOs will be responsible for the hard drive removal, recycling, destruction and/or disposal process. A waiver may be requested from DoIT's Enterprise Information Services to allow disposal of a device with a hard drive provided that the agency CIO provides justification for this variance as well as written certification that the included electronic media has been overwritten in accordance with U.S. Department of Defense media cleaning standards.

For situations in which the IT equipment 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.

SECTION 7: Network Security

State agencies own and operate a local area network infrastructure to support approved user applications and services. Agencies must ensure that all networks are protected from unauthorized access at all entry points. To help accomplish this, each agency must, at a minimum:

- Establish a process for restricting local network access to authorized devices only;
- Establish a process to protect from unauthorized dial-in access;
- Utilize the State approved banner text;
- Establish a process to ensure that all external IP connections are made through a firewall;
- Implement and monitor an Intrusion Detection Systems (IDS) or Intrusion Prevention System (IPS);
- Establish a process to ensure that all Service Interface Agreements (SIAs) are managed in accordance with their IT Security Program and the State Policy;

- Establish a process to ensure that the same level of controls that exist on-site exist for users working remotely;
- Establish a process to prevent unauthorized active content from being loaded onto State IT equipment;
- Establish a process for ensuring that wireless network connections do not compromise the Agency's network;
- Establish a process for securing all Private Branch Exchanges (PBXs);
- Establish a process to prevent unauthorized networks to access VoIP networks.

7.0 Local Network Access

- Network devices shall be configured and maintained so as to not cause network performance degradation, not cause excessive, unwarranted traffic flows, and be suitably hardened against network security threats
- Authorized users shall not connect devices which are not the property of, nor under the control of the Agency, to the Agency's computing resources without prior written approval by the CIO or other delegated authority of the Executive Departments or Independent State Agency. If approved, the user may be granted restricted network access rights and is required to provide protections equivalent to the Agency's protection of its own equipment
- Authorized users shall adhere to the Agency's Policy on Acceptable Use of the Information Infrastructure
- In accessing the network, authorized users shall adhere to, and network connecting devices shall conform to, the policies set forth in this document

7.1 Dial-in Access

Dial-up refers to connecting a device to a network via a modem utilizing a public telephone network. The following controls for dial-in users must be implemented:

- Unique network access user ids different from their application or network user id;
- A minimum prohibition of answer or pickup until after the sixth (6th) ring;
- Access privileges must be prohibited to any applications except those expressly required (i.e. cannot grant access to entire network, must be application specific);
- Annual review of access requirements;
- Remote user shall not store data unless the data can be protected from unauthorized access, modification, or destruction.

The following services are prohibited except where they are specifically approved by the Agency CIO or other delegated authority of the Executive Departments or Independent State Agency:

- Dial-in desktop modems;
- Use of any type of "remote control" product (e.g., PCAnywhere, GoToMyPC);
- Use of any network-monitoring tool.

7.2 Banner Text Policy

Banners are electronic messages that provide notice of legal rights to users of computer networks. State banners are used to generate consent to real-time monitoring and eliminate the "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network. The following is an example of the type of banner text that must be displayed at all system entry points and at all access points to servers, subsystems, etc... where initial user logon occurs.

“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.”

An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read. The banner is:

- Required for all mainframe, midrange, workstation, personal computer, and network systems;
- Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices;
- The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen. In such cases, this negative impact must be documented in the Agency’s IT Security Program.

7.3 Firewalls & Network Devices

Firewalls provide a layer of defense that protects local area networks from un-trusted (Internet) sources. State networks shall be protected by firewalls at identified points of interface as determined by system and data classification. Firewall implementation requirements;

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

7.4 Intrusion Detection Policy

Intrusion Detection/Prevention Systems provide a means for detecting suspicious behavior within the network, generating alerts and offering mitigation options. State networks shall be monitored by an IDS or IPS implemented at critical junctures. Host-based, network-based, or a combination of both may be utilized.

IDS/IPS implementation requirements;

- Default administrator username and password must be changed;
- Management access must be limited to appropriate personnel;
- System must be monitored and/or information logged 24x7x365;
- Signature-based solutions must be updated on a regular schedule;
- Each agency must establish a severity and escalation list based upon anticipated events that include immediate response capability when appropriate. These plans should be incorporated in the Agency’s IT Security Program.

7.5 Service Interface Agreements

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 non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system IT Security Certification and Accreditation package and in the IT System security plan. An SIA shall include:

- Purpose and duration of the connection as stated in the agreement, lease, or contract;
- Points-of-contact and cognizant officials for both the State and non-State organizations;
- Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations;
- Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection;
- Requirements for notifying a specified State official within a specified period of time of a security incident on the network, with the recommended time within 4 hours of the incident;
- A provision allowing the State to periodically test the ability to penetrate the non-state network through the external network connection or system.

7.6 Remote Access

This policy applies to all employees, contractors, vendors and agents with a computer used to connect to an agency network (including the connections used) to perform work on behalf of the agency including reading or sending email and viewing intranet web resources.

Storage of confidential information on any non-state owned device is prohibited. Confidential information may not be stored on any state owned portable device without prior written approval from agency Secretary (or delegated authority). Approved storage on any portable device must be encrypted.

It is the responsibility of employees and contractors with remote access privileges to ensure that their remote access connection is given the same consideration as the user's on-site agency connection. All remote access users are expected to comply with agency policies, may not perform illegal activities, and may not use the access for outside business interests. The minimum requirements for a remote access solution are;

- Equipment that is used to connect to an agency's network must meet the minimum security requirements of agency-owned equipment.
- Remote access must be strictly controlled with unique user credentials.
- Remote access passwords are to be used only by the individual to whom they were assigned and may not be shared.
- All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption.
- Split-tunneling or dual homing is not permitted at any time.

7.7 Active Content

Active content or mobile code refers to electronic documents that can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. Active content technologies allow code, in the form of a script, macro, or other kind of portable instruction representation, to execute when the document is rendered. Like any technology, active content can be used to deliver essential services, but it can also become a source of vulnerability for exploitation. Agencies should understand the concept of active content and how it affects the security of their systems.

Security is inversely related to complexity – the more complex a system, the more difficult it is to secure. Therefore, the functionality of a system should be reduced to the minimum needed to carry out its operation. Administrators should remove unnecessary applications and program components to reduce complexity and shut off possible avenues of attack.

- Procedures shall be implemented to remove any unnecessary software including development tools not needed in providing Web services.
- Server-side scripts must constrain users to a small set of well-defined functionality and validate the size and values of input parameters.
- Scripts must be run only with minimal privileges (i.e., non-administrator).
- Create and distribute active content documents only after carefully considering the risk and benefits.
- Agencies shall obtain all software through approved distribution channels.
- Institutionalize how needed plug-ins and other software code are obtained from software manufactures, evaluated, and distributed throughout the agency.
- Administrators must become knowledgeable of the security settings of desktop applications and turn off unneeded functionality such as unnecessary plug-ins or ActiveX controls.
- Keep systems current with the latest software upgrades and patches that address security vulnerabilities in desktop applications, such as Web browsers, readers, email clients, and other critical software.
- Evaluate and install anti-malware software, firewalls, active content filters, and dynamic behavior monitors according to agency security requirements. Keep these products upgraded to the latest version.
- Educate users to not peruse active content or run downloaded software from untrusted sources. Enable ActiveX code only from trusted Web sites that require its use.
- Educate users to not open active content documents or execute any email attachments without first verifying them with the sender.
- Disable JavaScript and any other active content processing capabilities within email desktop applications that are capable of handling HTML or other markup language encoded messages.
- Administrators must keep informed of latest security advisories from the United States Computer Emergency Readiness Team (US-CERT) and the Computer Emergency Response Team (CERT) Coordination Center, and subscribe to security mailing lists.
- Administrators must periodically cross-check products against published lists of known vulnerabilities, such as the National Vulnerability Database (NVD) that provide pointers to solution resources and patch information.
- Know who to contact and what steps to take when discovering evidence of an intrusion.

7.8 Wireless

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 so that the SSID broadcast range does not exceed 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

7.9 Private Branch Exchange (PBX)

If PBX processors require remote vendor maintenance via a dial-in telephone line the following controls must be in place:

- A single dedicated telephone line that disables access to the public-switched telephone network;
- An automated audit trail;
- Encryption of transmissions;
- Access controls.

SECTION 8: Access Control

All Agencies must ensure that information is accessed by the appropriate persons for authorized use only. To help accomplish this each agency must establish at a minimum the following:

- An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system;
- An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of “least possible privileges” and “need-to-know”;
- An audit trail process to ensure accountability of system and security-related events;
- A process for ensuring that all systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, this capability must be enabled at all times;
- A review process of security audit logs, incident reports and on-line reports at least one (1) time per business day using automated tools to facilitate the review where possible;
- An investigation process for any unusual or suspicious items, which will incorporate reporting the incident to DoIT Enterprise Information Services’ Security Team.
- The processes to establish, manage, and document user id and password administration;
- A review of access privileges on an annual basis;
- A process for protecting confidential information;
- A process for explicitly authorizing access to confidential information;
- A process for documenting and escalating all instances of non-compliance with the State IT Security Policy;
- A segregation of the functions of system administration and security administration to provide separation of duties;
- Independent audits of agency security administrators’ security transactions.

8.0 Authentication

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

8.1 Password Construction Rules and Change Requirements

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 passwords at regular intervals;
- Password reuse must be prohibited by not allowing the last 10 passwords to be reused with a minimum password age of at least 2 days;
- Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
- Automated controls must ensure that passwords are changed at least as frequently as every ninety (90) days for regular users, forty-five (45) days for power users, such as network and database administrators;
- Passwords older than its expiration date must be changed before any other system activity is performed;
- User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts while allowing a minimum of a ten (10) minute automatic reset of the account;
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

8.2 Authorization

All Agencies must have the following authorization controls implemented:

- A documented process to ensure that access privileges are verified at least annually;
- An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity;
- A documented process to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hours of the change;
- A documented process to ensure that physical and logical access is immediately disabled upon a change in employment status where appropriate;
- An automated process to ensure that user ids are disabled after sixty (60) days of inactivity unless they are extended through the explicit approval of the Information Custodian (Note: Functional ids may be exempted from this requirement);
- A documented process to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use;
- A process/system to ensure that access privileges are traceable to a unique user id;
- An automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon.

8.3 Audit Trail

The following minimum set of events/actions must be logged and kept as required by State and Federal laws/regulations:

- Additions, changes or deletions to data produced by IT systems;
- Identification and authentication processes;
- Actions performed by system operators, system managers, system engineers, technical support, data security officers, and system administrators;
- Emergency actions performed by support personnel and highly privileged system and security resources.

The audit trails must include at least the following information:

- Date and time of event;
- User id of person performing the action;
- Type of event;
- Asset or resource name and type of access;
- Success or failure of event;
- Source (terminal, port, location, IP address) where technically feasible.

8.4 Violation Log Management and Review

The Information Custodian must review all violations within one business day of a discovered occurrence. Automated tools are recommended when performing this review whenever possible. At a minimum the following events should be reviewed:

- Two (2) or more failed attempts per system day to access or modify security files, password tables or security devices;
- Disabled logging or attempts to disable logging;
- Two (2) or more failed attempts to access or modify confidential information within a week (5 business days);
- Any unauthorized attempts to modify software or to disable hardware configurations.

SECTION 9: Communication and Operations Management

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

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code. Although the elements are described in terms of the technologies needed and/or used for system and communication protection it is really the processes that administer and monitor the technologies that assure the required level of security.

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

Operations management covers IT assets throughout their lifecycle. Thus, it is greater than the cost of just purchasing assets, and includes all ongoing maintenance, security, monitoring and problem resolution. The overall goal of operations management is to lower the total cost of ownership of all organizational devices, from enterprise servers to mobile devices attached to the network, while keeping the environment secure.

Proper operations management safeguards all of the organization's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers. The method of protection used should not make working within the agency's computing environment an onerous task, nor should it be so flexible that it cannot adequately control excesses. Ideally, it should obtain a balance between these extremes, as dictated by the agency's specific business needs.

This balance depends, at least in part, on two items. One is the value of the data, which may be stated in terms of intrinsic value or monetary value. Intrinsic value is determined by the information's criticality and sensitivity — for example, health- and personal-related information may have a high intrinsic value. The monetary value is the potential financial or physical losses that would occur should the information be breached or violated. The second item is the ongoing business need for the information, which is particularly relevant when continuous availability (i.e., round-the-clock processing) is required.

Minimum agency requirements include;

- Implement cryptographic solutions (encryption) when the confidentiality or sensitivity of information must be maintained while a message is in transit between computing devices and when confidential or sensitive information is stored in a file or database.
- Deploy and routinely update appropriate anti-virus, anti-spyware and file extension blocking solutions at the gateway entry points and on the desktop and server systems to prevent these systems from being compromised.
- Ensure a firewall or other boundary protection mechanism is in place and has the ability to (1) evaluate source and destination network addresses, and (2) compare the request (including destination ports) to predefined access control lists for filtering purposes.
- Deploy appropriate Intrusion Detection System and Intrusion Prevention System (IDS/IPS) solutions at the correct network location(s) and monitor to detect when the agency is under attack so an effective detection and defense strategy can be deployed.
- Implement an appropriate change management process to ensure changes to systems are controlled.
- Provide for separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
- Establish procedures to implement an agreed backup policy and strategy, including the extent (e.g., full or differential/incremental), frequency, offsite storage, testing, physical and environmental protection, restoration, and encryption.
- Secure certain internal data and systems (Personnel Services, for instance) from other data and systems on the networks.
- Do not place confidential or sensitive data on any application servers, database servers, or infrastructure components that require direct access from the Internet. Components that meet these criteria must be placed behind a de-militarized zone (DMZ) where they are not accessible from the Internet and can only interact with DMZ components through a firewall.
- Establish appropriate procedures to protect documents, computer media, information/data, and system documentation from unauthorized disclosure, modification, removal, and destruction, including suitable measures to properly dispose of media when it is no longer needed.
- Establish procedures and standards to protect information and physical media containing information in transit, including using facsimile machines, exchange agreements between the agency and external parties, transportation of physical media, and monitoring (e.g., audit logging, monitoring system use.)
- Implement appropriate levels of security monitoring including intrusion detection, penetration testing, and violation analysis.
- Perform reviews of audit trails on a regular basis to alert an agency to inappropriate practices.

- Ensure preventive or detection controls are in place to decrease or identify the threat of unintentional errors or unauthorized users accessing the system and modifying data.
- Implement appropriate retention policies as dictated by the agency's policies, standards, legal and business rules.
- Implement appropriate documentation such as security policies and procedures, business contingency plans, disaster recovery plans, and incident response plans, including a plan for cyber attacks, such as a denial of service attack.

SECTION 10: Policy Violations

Executive Departments and Independent State Agencies will determine the appropriate corrective measures necessary to immediately remedy the violation. Disciplinary action, up through termination, may be warranted in cases of severe negligence.

APPENDICES

Appendix A: Computer Security Incident Handling Form

COMPUTER SECURITY INCIDENT HANDLING FORM

INCIDENT IDENTIFICATION

Incident Detector's Information:

Name:

Title:

Agency:

Phone:

E-mail:

Address:

Date and Time Detected:

Type of Incident Detected:

Denial of Service

Unauthorized Use

Unauthorized Access

Malicious Code

Probe

Other _____

How was the incident discovered?

Describe the incident characteristics:

What is the impact to your organization?

How can this type of incident be prevented?

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.
Cable Modem	Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet.
Dial-in Modem	An external device or internal electronic circuitry used to transmit and receive digital data over a communications line normally used for analog signals.
DMZ	Also known as a Data Management Zone or demarcation zone, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a DoIT-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.
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. Refer to DoIT's Acceptable Encryption Policy for more information.
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.
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.
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: <ul style="list-style-type: none"> • 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.
Remote Access	Any access to DoIT's corporate network through a non-DoIT controlled network, device, or medium.
Sensitive	Information that, if divulged, could compromise or endanger the citizens or assets of the State.

SNMP	Simple Network Management Protocol is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
Split-tunneling	Simultaneous direct access to a non-DoIT network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DoIT's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.
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.
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