Information Technology Security Policy for Maryland Insurance Administration

Version 4.1
July 16, 2015

INSURANCE ADMINISTRATION

200 St. Paul Place
Baltimore, MD 21202
410-468-2000
1-800-492-6116
www.mdinsurance.state.md.us

LARRY HOGAN, GOVERNOR *BOYD K. RUTHERFORD, LT. GOVERNOR*

AL REDMER, JR., COMMISSIONER
NANCY GRODIN, DEPUTY COMMISSIONER

TABLE OF CONTENTS

SECTION 1: PURPOSE AND INTRODUCTION

Effective July 1, 2014, the State Government Article requires State agencies to adopt procedures to protect an individual's personal information from unauthorized access. See State Government Article, Annotated Code of Maryland, Section 10-1304. This new legislation is intended to protect all "personal information" as defined by State Government Article Section 10-1301.

The purpose of this Policy is to set forth the security requirements that the Maryland Insurance Administration (MIA or Agency) must meet in order to protect the confidentiality, integrity and availability of personal information that is electronically generated, received, stored, printed, scanned, filmed or typed by the MIA. This Policy establishes a minimum standard and a consistent approach for information technology (IT) security.

This Policy is in addition to, and not in replacement of, the Statewide Information Technology Security Policy established by the Maryland Department of Information Technology (DoIT). The standards set forth in this Policy were drafted in accordance with Version 3.1 of that policy, dated February 2013. At the direction of DoIT, the MIA has adopted the National Institute of Standards and Technology's[1] (NIST) information security related standards and guidelines in the context of its mission, business responsibilities, operational environment, and unique organizational conditions.

1.1 Scope

This Policy pertains to all information within MIA systems that is processed, stored or transmitted by any means. This includes: electronic information, information on paper and information shared orally or visually.

As used in this Policy, the terms "IT system" or "electronic communications system" includes, but is not limited to, hardware, software, equipment, storage media, electronic mail, telephones (landlines and mobile), voice mail, mobile messaging, Internet access, and facsimile machines, regardless of whether the system is hosted in the MIA data center or at a third party offsite location.

"Personal information" means: an individual's first name or first initial and last name, personal mark or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- A Social Security Number;
- A driver's license number, state identification card number, or other individual identification number issued by a unit;

[1] NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's 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.

- A passport number or other identification number issued by the United States Government;
- An individual taxpayer identification number or;
- A financial or other account number, a credit card number, or a debit card number that in combination with any required security code, access code, or password, would permit access to an individual's account.

See State Government Article Section 10-1301 (c) for reference.

1.2 Objectives

IT systems are critical to the services that the MIA provides for consumers, producers, insurance companies, and other regulated individuals and entities, as well as to state and federal government entities. This Policy sets forth security requirements that, when implemented, will help to ensure the security, confidentiality and integrity of personal information that is collected, stored, maintained, transmitted or otherwise processed through the MIA's IT systems.

This Policy defines the minimum standards and requirements to which each MIA business unit, including employees and contractors, must adhere. The MIA's business units are as follows:

- Commissioner's Office;
- Administration Unit;
- Compliance and Enforcement;
- Consumer Education and Advocacy;
- Examination and Auditing;
- Fraud;
- Life and Health;
- Market Conduct;
- Office of the Chief Actuary; and
- Property and Casualty.

The primary objectives of the MIA IT Security Policy are:

- to establish a secure environment for the processing of data;
- to reduce information security risk; and
- to communicate the responsibilities for the protection of personal information.

The provisions of this Policy apply to all business units in the MIA unless an exception has been approved in writing by the Commissioner.

SECTION 2: ROLES AND RESPONSIBILITIES

This Policy sets forth the minimum level of responsibility for the following:

- MIA Senior Management Staff;
- MIA Management Information Systems (MIS) Department;
- MIA Employees (permanent and temporary);
- MIA Contractors.

2.1 MIA Senior Management Staff

Security of personal information is an Agency responsibility shared by all members of the MIA's senior management team. MIA Senior Management Staff shall provide clear direction and visible support for Agency security initiatives. Senior Management Staff are responsible for:

- initiating measures to assure and demonstrate compliance with the security requirements set forth in this Policy;
- implementing and maintaining the MIA's information security policy within their business unit;
- ensuring that IT security is part of the planning and procurement process;
- complying with the requirements established by Section 10-1301 *et. seq.* of the State Government Article of the Annotated Code of Maryland;
- complying with the MIA's record retention policies; and
- performing as "business owners" (as defined in § 3.1 of this Policy) for the business unit's IT systems and data assets.

2.2 MIA Management Information Systems (MIS) Staff

The MIA's MIS Department is responsible for:

- developing, maintaining, and revising IT policies, procedures, and standards for the MIA;
- assuring the confidentiality, integrity, availability, and accountability of all personal information while it is being processed, stored, and/or transmitted through an electronic communication system;
- ensuring separation of duties and assigning appropriate system permissions and responsibilities for system users;
- participating in IT security control audits focusing on compliance with State and MIA IT security policies;
- determining the feasibility of conducting external and internal vulnerability assessments and penetration tests to verify security controls are working properly and to identify weaknesses; and
- developing, implementing and testing an IT Disaster Recovery Plan for business critical MIA Systems.

2.3 MIA Employees

All MIA employees, whether permanent or temporary, are responsible for:

- being aware of and complying with the MIA's IT security policy;
- using IT resources only for intended purposes as defined by State laws and the MIA's Electronic Communications and Electronic Communications Systems policy;
- being accountable for their actions relating to their use of all MIA IT systems and data; and
- reporting security incidents.

2.4 MIA Contractors

All MIA contractors are responsible for:

- being aware of and complying with the MIA's IT security policy;
- complying with the terms of their non-disclosure agreement and contract with the MIA;
- being accountable for their actions relating to their use of all MIA IT systems and data; and
- reporting security incidents.

All MIA contractors shall ensure that their employees, consultants, independent contractors and subcontractors also meet the above standards.

SECTION 3: ASSET MANAGEMENT

This section defines the asset management process the MIA shall use to identify and assess the acceptable risk to the MIA's IT systems and data assets. The MIA shall establish and maintain an inventory of IT systems and data assets and categorize the security risk associated with each asset. As an output of this process, the MIA shall identify the appropriate controls for reducing or eliminating security risks to IT systems and data assets. IT systems and data assets include:

- information assets (databases, data files, system documentation, user manuals, training materials, operational procedures, disaster recovery plans, archived information);
- software assets (application software, system software, development tools and utilities);
- physical assets (computer equipment, communications equipment and magnetic media); and
- services (computing services, communications services and general utilities).

3.1 Inventory of Assets

Compiling an inventory of IT systems and data assets is an important aspect of risk management. MIA business units shall participate in the identification, assessment, and security classification of their assets. Each IT system and data asset should be clearly identified and its ownership and security classification agreed and documented.

In assessing their inventory of IT systems and data assets, the business unit shall work with MIS to document the following:

- determine the appropriate asset category (information, software, service, physical);
- assign a unique asset name;
- provide a general description of the asset;
- identify the business owner (the MIA Senior Management Staff member for the business unit or their designee, responsible for approving access and permissions to the IT system or data asset);
- determine the appropriate security classification and risk categorization;
- define guidelines for marking and distribution;
- identify the physical location of the asset (the data center hosting the asset);
- identify the server name (if applicable), and/or the database type and name (if applicable);
- identify the date created; and
- identify the data retention needs of the asset (when to archive or purge data) in accordance with established Agency record retention policies.

Once documented, the business unit inventory of assets shall be shared with MIS to establish, implement and maintain controls commensurate with the value and security risk associated with each asset**.** The business unit inventory of assets shall be reviewed annually to determine if changes are required, and updated accordingly.

3.2 Information Security Classification

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

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

1) public; or
2) confidential.

Public information is information that is not protected information, and which can freely be given to anyone without concern for potential impact to the State of Maryland, its employees or citizens.

Confidential information is information that is in the possession of the MIA which has been designated non-public, either by operation or law or by decision of the Associate

Commissioner for an MIA business Unit, and includes personal information (as defined in § 1.1 of this Policy).

Information that is confidential by operation of law includes information that is protected by a legal privilege, such as attorney-client privilege, executive privilege[2], or the attorney work product doctrine, as well as information for which disclosure is barred by contract, State or Federal law, or judicial order.

Sometimes disclosure of information may not be barred by law, but the information is of a sensitive nature and public disclosure may either compromise or cause harm to the State or to the original owner of such information and the Public Information Act (PIA) permits non-disclosure. For example, the PIA permits non-disclosure of licensing related examination questions to persons who have not taken the exam if the custodian believes disclosure would be contrary to the public interest.

Information shall be classified as it is received, created or distributed by the business unit. If an MIA employee is uncertain of the classification of a particular piece of information, the employee should contact the Associate Commissioner of their business unit, for clarification.

All personal information on paper or removable media must be clearly marked "Confidential" and will be subject to the marking and distribution guidelines (as defined in § 4.2.2 of this Policy).

[2] The doctrine of executive privilege protects from disclosure confidential, advisory documents and records, as well as deliberate communications that include or reflect internal agency deliberations, opinions and recommendations, or otherwise reveal the decision-making process of the Agency. It may apply, but is not limited to, internal or interagency document or records:

- relating to budgetary and fiscal analysis, policy papers and recommendations made by the Agency or by any person working for the Agency;
- provided by another agency to the MIA in the course of the Agency's exercise of its responsibility to prepare and monitor the execution of the annual budget;
- relating to the Agency's discretionary decisions in a procurement, such as an evaluation of committee member's notes;
- that are draft Orders, Bulletins or Consent Agreements which have not yet been finalized and issued;
- that are draft legislation or regulations.

If you believe that certain information is protected by executive privilege, you should consult with the Office of the Attorney General before categorizing it as "confidential".

SECTION 4: SECURITY CONTROLS

This Section defines requirements that must be met and controls implemented by the MIA to properly secure personal information. All MIA IT systems used for receiving, processing, storing and transmitting personal information must be secured in accordance with these requirements.

This framework categorizes security controls into three types:

- management;
- operational; and
- technical.

4.1 Management Level Controls

Management security controls focus on managing organizational risk and devising sufficient counter measures for mitigating risk to acceptable levels. MIA's management security controls include risk management, system security planning, and network services.

4.1.1 Risk Management

Risk Management refers to the process of identifying, assessing and mitigating risks. The MIA shall use risk assessment to determine the risk associated with IT systems and data assets and the extent of any potential threat. Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing controls. Controls are defined as processes and technologies designed to close vulnerabilities, maintain continuity of operations at specified performance levels, and achieve and document compliance with policy requirements. Security classification of assets and security risk categorization are essential components of risk management.

4.1.2 Risk Categorization

The security risk category determines the level of controls required to protect the IT system or data asset from a security breach. The MIA shall use three security risk categories: low; moderate; or high[3], as defined in the table on the following page. The categories are based on the potential impact to the MIA should a breach of security occur which affects the integrity, confidentiality, accessibility or availability of the Agency's IT system or data asset. Business units should review risk categorizations annually to determine if changes are required, and update accordingly.

[3] These security risk categories are based on the information technology assets security categorizations described in the Federal Information Processing Standards (FIPS) Publication 199.

Security Risk Categories

Risk Category	Effect of security breach on MIA operations, assets, or individuals	Factors to Consider
Low	nominal or limited	• information is not personal information; • breach would cause a degradation in mission capability to an extent and duration that the MIA is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; • breach would result in minor damage to agency assets; • breach would result in minor financial loss; • breach would result in minor harm to individuals.
Moderate	serious, adverse effect	• information is personal information; • breach would cause a significant degradation in mission capability to an extent and duration that the MIA is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; • breach would result in significant damage to agency assets; • breach would result in significant financial loss; • breach would result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	a severe or catastrophic adverse effect	• information is personal information. • breach would 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; • breach would result in major damage to agency assets; • breach would result in major financial loss; • breach would result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Determining the security categorization (Low, Moderate or High) for an IT system or data asset requires consideration of the sensitivity of the data, and the potential impact

values (confidentiality, integrity and availability). If information is marked, or should have been marked "confidential" information, it must be categorized, at minimum, as a moderate risk.

4.1.3 System Security Planning

The MIS Unit shall review the MIA's IT Security Policy annually to assess whether changes are required, and update accordingly. In addition, MIS shall document a system security plan describing the security requirements, current controls and planned controls, for protecting agency IT systems and data assets. The system security plan shall be reviewed annually and updated as necessary, to account for significant changes in the security requirements and controls deemed necessary to protect the MIA's IT systems and data assets.

4.1.4 Network Services

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

External network connections shall be permitted by MIS only after all approvals consistent with this policy and other laws or regulations are obtained and documented.

4.2 Operational Level Controls

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.

4.2.1 Awareness and Training

The MIA shall ensure that all employees and contractors have reviewed and acknowledged the MIA Information Technology Security Policy and the Agency's Electronic Communications and Electronic Communications Information Systems Policy before authorizing access to IT systems. Human Resources will collect and maintain acknowledgement forms from every employee. The Procurement Officer will obtain a signed non-disclosure agreement from each contractor who will have access to personal information.

4.2.2 Guidelines for Marking and Distributing Information

MIA business units shall comply with the following guidelines in handling information that is printed or stored on removable media:

4.2.2.A Public Information

Information that has no restrictions on disclosure is subject to the following standards:

- Marking: No marking requirements.
- Access: Unrestricted.
- Distribution: No restrictions.
- Storage: Standard operating procedures based on the highest security category of the information recorded on the media.
- Disposal/Destruction: In compliance with the MIA's document retention policy.
- Penalty for deliberate or inadvertent disclosure: Not applicable.

4.2.2.B Personal Information

Each MIA Business Unit shall determine the appropriate standards for marking and distributing personal information based on the security risk categories (as defined in § 4.1.2 of this Policy) using the following as a guideline:

- Marking: Personal information (as defined in § 1.1 of this Policy) is to be clearly identified as "Confidential" information.
- Access: Only MIA employees with a need to know; MIA contractors or other individuals or entities that the business owner has determined have a mission-essential need to know and the individual or authorized entity designee has signed a non-disclosure agreement.
- Distribution: Determined by the Associate Commissioner of the MIA Business Unit, based on the defined security risk category (low, moderate or high) of the information being distributed. Examples:
  - Delivered direct – signature required, envelopes stamped Confidential, or delivered by approved private carriers; or
  - Sent electronically via encrypted email or MIA approved electronic file transmission method.
- Storage:
  - Physically control access to system media (paper and digital) and protect personal information using encryption technologies and/or other substantial mitigating controls, such as password protection, limited access, network security event monitoring and database change monitoring;
  - Storage is prohibited on mobile devices, non-agency owned devices, and publicly accessible systems unless the Commissioner or her designee has granted prior written approval;
  - Approved storage on portable devices or publicly accessible systems must be encrypted; and
  - Keep personal information 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: Deposit paper containing personal information in a locked paper bin designated for shredding; electronic storage media is sanitized or destroyed using MIA's approved method (as defined in § 4.2.6B of this Policy).

The penalty for deliberate or inadvertent disclosure of personal information can range from administrative actions to adverse personnel actions up to termination of employment. Deliberate, unauthorized disclosure of personal information may also result in civil and/or criminal penalties.

4.2.3 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). These procedures will be reviewed annually to determine if changes are required, and updated accordingly.

All default system administrator passwords must be changed upon implementation of the system. MIS shall implement and maintain an appropriate configuration management process to ensure changes to IT systems are controlled by:

- developing, documenting and maintaining secured baseline configurations;
- developing, documenting and maintaining an inventory of the components of business critical systems and relevant business ownership information;
- configuring systems to provide only essential capabilities;
- configuring the security settings of IT products to the most restrictive mode consistent with operational requirements;
- analyzing potential security impacts of changes prior to implementation;
- authorizing, documenting and controlling system level changes;
- restricting access to system configuration settings and providing the least functionality necessary;
- prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing or transmitting personal information; and
- maintaining backup copies of hardened system configurations.

4.2.4 Contingency Planning

As an adjunct to and in support of the MIA COOP planning, the MIA shall develop, implement, and test an IT Disaster Recovery (DR) plan for all systems determined to be "business critical." Systems that are business critical are applications and services that are necessary for the MIA to conduct operations. Creation, maintenance, and annual testing of a DR plan will minimize the impact of recovery and loss of IT systems caused by events ranging from disruption of a single business system to a disaster impacting the entire MIA data center.

Primary components of an IT DR Plan include:

- identification of a disaster recovery team and emergency contact information;
- definitions of recovery team member responsibilities;
- documentation of each business critical system including:

    - System name;
    - Business owner;
    - Description of system;
    - Server hardware;
    - Operating system;
    - Data base;
    - Supporting network infrastructure and communications; and
    - System restoration procedures;

- system restoration priority list;
- description of current system back-up procedures;
- description of back-up storage location; and
- identification of disaster recovery site including contact information.

Once documented, the MIA DR Plan will be reviewed annually to determine if changes are required, and updated accordingly.

4.2.5 Incident Response

Incident management refers to the process of identifying, responding to and managing information security incidents. MIA has adopted a State-mandated common set of terms that provides a platform for data collection and analysis.

All MIA employees and contractors are expected to report security incidents promptly, and within the designated timeframe, by using the MIA Security Incident form available on the Technology page of the MIA Intranet site or by calling the MIS Help Desk. After verifying that an incident has occurred, MIS will classify the functional, information and recoverability impact of the incident and if appropriate, report the incident to DoIT.

MIA employees and contractors shall utilize the following security incident categories and report events within the designated timeframe:

Security Incident Categories

Category	Incident Type	Description	Response
CAT 1	Unauthorized Access	An individual or contractor gains logical or physical access without permission to the MIA's network, system, application, data, or other resource	Report to MIS
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 type of activity includes being the victim of a denial of service, or participating in it. If an individual is unable to access an application they normally have access to, they should assume that a denial of service has occurred.	Report to MIS
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. If an individual observes something odd after opening an email attachment or clicking on a link, they should assume malicious software has been installed.	Report to MIS
CAT 4	Improper Usage	A person violates acceptable computing use policies as defined in the MIA's Electronic Communications and Electronic Communications Systems Policy.	Report to Supervisor

4.2.6 Media Protection and Management

No IT equipment shall be released from the MIA's control until the data storage devices have been removed and rendered inoperative, or removable media has been destroyed or conditioned so data are unrecoverable. This Policy applies to all electronic storage media equipment that is owned or leased by the MIA including, but not limited to: desktop and laptop computers, servers, Blackberries, iPads, multi-function printers/copiers, flash/thumb drives and other portable storage devices.

4.2.6.A Marking Media

All media that contains personal information (as defined in § 1.1 of this Policy) including removable media (CD's, magnetic tapes, external hard drives, flash/thumb drives, and DVD's) and information system input and output (reports, documents, data files, back-

up tapes) shall be clearly labeled “Confidential”. MIA shall restrict access to system media containing personal information to authorized individuals. MIA employees and contractors shall not store data on electronic media that cannot be adequately secured against unauthorized access.

4.2.6.B Sanitization Standards

IT equipment including, but not limited to, desktop computers, laptop computers, servers, and multi-function printers/copiers, shall not be released from the MIA’s control until the equipment is sanitized using the following procedures:

1) Equipment returned to vendor/s for warranty repair or replacement:

    - MIS shall remove hard drive/s from device/s before equipment leaves the control of MIA.

    - If a hard drive is being replaced, MIS shall degauss the hard drive/s prior to returning drive to vendor for replacement.

2) Equipment being transferred to surplus due to end of life or no longer needed:

    - MIS shall remove hard drive from all devices and document the A-Tag on the hard drive.

    - MIS shall record the following information on the Inventory Transfer Sheet:

        - Inventory Number (A-Tag);

        - Equipment Description;

        - Manufacturer and Model Number;

        - Serial Number of Equipment; and

        - Hard Drive Serial Number.

    - Two technicians must check hardware devices to verify that drives have been removed and initial each device on the Inventory Transfer Sheet.

    - Deliver equipment and Inventory Transfer Sheet to Fiscal for disposal of equipment.

    - Store hard drive/s in secure storage room until destruction is scheduled with authorized vendor.

    - Destroy hard drives by shredding. If shredding is performed by a third party, a Certificate of Destruction shall be obtained.

4.2.7 Data Center Security

Physical access to IT processing equipment, media storage areas, 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.

Access to the MIA data center and MIS secured work areas shall be limited to those employees and contractors who have legitimate business responsibilities in those areas. Authorization shall be based on frequency of need for access and approval by either the MIA Commissioner or CIO, or their designees.

The MIA is responsible for ensuring that:

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

4.2.8 System and Information Integrity

The MIA shall protect against malicious code (*e.g.*, viruses, worms, Trojan horses) by implementing anti-virus, anti-malware solutions that, to the extent possible, include 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 IT systems and/or personal information.

The MIA shall restrict access to IT systems to authorized personnel responsible for receiving, processing, storing, or transmitting personal information. The MIA shall receive and review security alerts and advisories on a regular basis and take appropriate actions in response. The MIA shall identify, document and correct IT system vulnerabilities.

4.3 Technical Level Controls

Technical security controls focus on operations executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system.

4.3.1 Access Control Requirements

The MIA shall manage user accounts, including activation, deactivation, changes and audits to IT systems and network files. The MIA shall ensure that only authorized individuals have access to personal information and that such access is strictly controlled.

The MIA shall ensure that IT systems enforce separation of duties through assigned access authorizations and enforce the most restrictive access capabilities required for specified tasks.

The following warning shall be displayed on the MIA network logon screen before system access is granted:

> *"Access to this system is restricted to authorized users only and limited for acceptable uses as defined in the MIA's Electronic Communications and Electronic Communications Systems Policy. 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."*

The MIA shall authorize, document and monitor all remote access capabilities used on IT systems. Remote access is defined as any access to an MIA information system by a user communicating through an external network, for example: the Internet or a Virtual Private Network (VPN).

All remote access connections must utilize some form of encryption for transmission of data and authentication. Personal computers and mobile devices that are not the property of, or under the control of the Agency, may not be used to access the MIA network.

4.3.2 Identification and Authorization Control Requirements

MIA IT systems must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts, and validate users with standard authentication methods such as passwords, tokens, smart cards, or biometrics.

The MIA's user account management practices include the following:

- obtaining authorization from appropriate officials to issue user accounts to intended individuals;
- disabling user accounts when no longer needed; and
- developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by an IT system.

IT systems shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

4.3.3 User Authentication and Password Requirements

All users of the MIA network shall be uniquely identified with a user name and password.

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.

All passwords should be treated as sensitive, confidential Agency information. MIA employees shall refer any person demanding a password to this MIA IT Security Policy or to the MIS Help Desk (410.468.2088).

MIA employees shall not use the "Remember Password" feature of applications or browsers (*e.g.*, Internet Explorer, Outlook, Chrome). MIA employees shall not document passwords and store them in their office or laptop bag. MIA employees shall not store passwords in a file on any computer system or mobile device that does not provide encryption.

If an account or password is compromised, MIA employees shall report the incident promptly using the MIA Security Incident Form or contact the MIS Help Desk (as defined in § 4.2.5 of this Policy).

SECTION 5: CLOUD COMPUTING TECHNOLOGIES

MIA requires contractual assurances that security controls are in place for cloud-based applications that are commensurate with or surpass those used if the applications were hosted in the MIA data center. All contracts or memoranda of understanding entered into for cloud-based applications must incorporate a Non-Disclosure Agreement, and require, at minimum, compliance with the MIA's and the State of Maryland's IT Security Policies.

SECTION 6: MOBILE DEVICES

Laptops, tablets, flash drives and mobile communication devices have become very popular in the work place 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.

The purpose of this Policy is to prevent unauthorized disclosure of personal information, reduce the risk of spreading viruses or malware and prevent unauthorized access to MIA computers and information infrastructure.

6.1 MIA Issued Mobile Devices

As a matter of policy and best practice, personal data should not be stored on a mobile device. MIA business requirements may, on occasion, justify storing personal data on mobile computing devices. In these cases, the following standards must be applied:

- all mobile devices shall be password protected;
- all mobile devices shall provide full disk encryption capabilities;
- all mobile devices shall have timeout/locking features and device erase functions (including removable memory) enabled;
- all mobile devices shall have anti-virus and/or firewall protection installed;
- all mobile device operating system and application security patch installation shall be up to current agency standards;
- all vendor recommended patches, hot-fixes or service packs shall be installed prior to deployment and processes shall be in place to keep system hardware, operating system and applications current based on vendor support recommendations;
- mobile device options and applications that are not in use shall be disabled;
- proper asset management procedures shall apply to all mobile devices;
- protected information shall 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 connect to the MIA network.

The physical security of MIA issued mobile devices is the responsibility of the employee to whom the device has been assigned. If an MIA issued mobile device (laptop, flash drive or cell phone) is lost or stolen, the employee is responsible for promptly reporting the incident to their Supervisor and the MIS Help Desk.

6.2 Contractor Owned Mobile Devices

MIA business requirements may on occasion require contract resources to supplement a business team. Contract resources shall be notified during contract negotiation of MIA requirements for laptops and mobile devices, and non-disclosure agreements shall be signed as part of the vendor's contract with the MIA.

Contract resources who require remote access to the MIA network or systems will rely on an MIS installed Virtual Private Network (VPN) capability. The following standards must be met for mobile devices owned by contract resources before a VPN connection to the MIA environment will be established:

- all mobile devices shall be password or PIN protected;
- all mobile devices shall provide full disk encryption capabilities;
- all mobile devices shall have timeout/locking features and device erase functions (including removable memory) enabled;
- all mobile devices shall have anti-virus and/or firewall protection installed;

- all mobile device operating system and application security patch installation shall be up to current MIA standards; and
- whenever possible, mobile devices shall be scanned for viruses/malware before they connect to the MIA network.