	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<i>Policy: Information Security Policy</i>		
	<i>Originator: Information Technology</i>		
	Policy Number	Effective Date	Revision Date
137.08	November 7, 2016	December 21, 2018	

**Purpose:** The protection of private health information (PHI) and personally identifiable information (PII) is a priority of the Maryland Institute for Emergency Medical Services Systems (MIEMSS). The privacy and security of MIEMSS information and information systems is a critical part of normal business practices and is the responsibility of every MIEMSS employee.


- All persons with access to MIEMSS data and information systems are responsible for protecting PHI and PII from unauthorized access, modification, disclosure, and destruction.
- This policy sets forth the basic requirements for PHI and PII in accordance with the of the Maryland Department of Information Technology (DoIT) Security Policy <http://www.doit.maryland.gov/support/pages/securitypolicies.aspx>

## 1) Definitions

- a) **"User/MIEMSS Employee" (hereinafter "user")** means all employees and MIEMSS contract employees.
- b) **"Equipment"** means all workstations, servers, specialized lab diagnostic equipment containing any form of embedded memory, laptops, tablets, portable communication devices, multi-function printers/copiers, and environmental or process control equipment.
- c) **"Encryption"** means encryption equivalent to or exceeding Advanced Encryption Standard 256 (AES 256).
- d) **"Media"** means all removable media, CDs, magnetic tapes, external hard drives, flash/thumb drives, DVDs, copier hard disk drives, and information system input and output (reports, documents, data files, back-up tapes at the employee's location or those sent offsite).
- e) **"Protected Health Information" of PHI** means Protected Health Information as defined by 45 CFR 160.103 and generally refers to health information which reveals the identity of the patient or from which the identity of the patient can be determined.
- f) **"Personal Information/Personally Identifiable Information" or PI/PII hereinafter PII** means information that identifies an individual including an individual's address, driver's license number or any other identification number, medical or disability information, name, photograph or computer generated image, Social Security number, or telephone number.
- g) **"Public information"** means information without any restriction on access.
- h) **"Restricted personal use"** means acceptable use that is not job-related.

## 2) Labeling

Media containing PHI and PII shall be clearly labeled "Confidential." Users shall restrict access to media containing PHI and PII to authorized individuals. Confidential materials in soft copy shall contain a cover sheet containing the word "**confidential**" in large font, e.g., 28 pt.

	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<b><i>Policy: Information Security Policy</i></b>		
	<b><i>Originator: Information Technology</i></b>		
	Policy Number	Effective Date	Revision Date
	137.08	November 7, 2016	December 21, 2018

**3) Email**

PHI and PII sent by email to addresses other than miemss.org shall be encrypted with agency approved encrypted electronic email or encrypted electronic file transmission method.

**4) Security of Media Containing PHI and PII.**

- a) Off-site storage of PHI and PII (electronic and paper) shall be approved in advance in writing by the MIEMSS Information Security Officer.
  - i) Examples: Backup tape storage, storage of paper-based patient care reports, etc.
- b) The use of equipment and media containing PHI and PII off-site must be reported to and approved by the employee's Immediate Supervisor.
  - i) Examples: Thumb Drives, DVDs, file folders, etc.

**5) Information Security Practices**


- a) Log in credentials shall not be shared with other persons.
- b) Workstations shall be protected with a password required screensaver and/or lock when not attended by User.
- c) Cell/smart phones, laptops, tablets, or other devices containing PHI and PII shall be password protected.
- d) Portable equipment shall be securely stored or locked down to immovable objects.
- e) All PHI and PII on devices and storage media shall be encrypted with agency approved encrypted electronic file method.
- f) Backup media and all portable storage media such as hard drives, flash media drives, diskettes, magnetic tapes, laptops, portable communication device, DVDs and CDs containing PHI and PII shall be physically secure and locked when unattended.
- g) Utilization of the remote access system requires the authorization of the employees Supervisor and the MIEMSS Information Security Officer per the MIEMSS Remote Access Policy.

**6) Personnel and Visitor Security Practices**

- a) All MIEMSS employees shall display a State issued picture employee Identification badge at all times while on duty.
- b) Visitors shall be issued and shall prominently display State or Agency issued identification at all times.
- c) Visitors shall be escorted by a MIEMSS employee when accessing secured areas (e.g., server rooms, communication rooms, areas with paper records, etc.)
- d) Access to secured areas shall be need based.

**7) Password Protection**

- a) All User's authorized to access PHI and PII or agency IT assets shall protect those assets by creating and utilizing strong passwords. Here are a few key considerations:

	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<i>Policy: Information Security Policy</i>		
	<i>Originator: Information Technology</i>		
	Policy Number	Effective Date	Revision Date
137.08	November 7, 2016	December 21, 2018	


- i) Strong passwords will have the following characteristics.
  - (1) Contain a minimum of 8 alphanumeric characters.
  - (2) Contain both upper and lower case letters.
  - (3) Contain at least one number (for example, 0-9).
  - (4) Contain at least one special character (for example, @!\$%^&\*()\_+|~-=\{}[]:;'<>?,/).
- ii) Poor, or weak, passwords have the following characteristics, and shall not be used by any MIEMSS employee:
  - (1) Contain less than eight characters.
  - (2) Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
  - (3) Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
  - (4) Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
  - (5) Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
  - (6) Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
  - (7) Or some version of “Welcome123” “Password123” “Changeme123”
- b) **Do not** discuss passwords with others, write down and post conspicuously, or electronically store unless encrypted.
- c) **Do not** use the same passwords for work, home, and personal accounts. These account passwords **MUST** be different.
- d) **Do not** reveal your personal password over the phone to ANYONE.
- e) **Do not** use the "Remember Password" feature of applications and browsers.
- f) **Do not** reveal a password on questionnaires or security forms.
- g) If someone demands a password, have him or her contact the MIEMSS Department of Information Technology Help Desk at [computersupport@miemss.org](mailto:computersupport@miemss.org)
- h) If it is suspected that an account or password has been compromised, report the incident to MIEMSS Department of Information Technology Help Desk [computersupport@miemss.org](mailto:computersupport@miemss.org) and change the password immediately.

## 8) Personal Equipment

- a) As a general rule, personal equipment should not be used to conduct agency business. If the use of personnel equipment is required, see the MIEMSS Remote Access Policy 137.07 for guidelines and authorization.

## 9) Equipment or Media No Longer Required or In Use

- a) Users shall not throw out used agency equipment or media; Equipment and Media must be disposed of in an appropriate manner. Data storage devices (hard drives and other data

	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<i>Policy: Information Security Policy</i>		
	<i>Originator: Information Technology</i>		
	Policy Number	Effective Date	Revision Date
	137.08	November 7, 2016	December 21, 2018

storage devices and media) shall be rendered inoperative, or destroyed or conditioned so data is unrecoverable.


- b) Disposal of any media containing agency records shall be in compliance with the agency's document retention policies and litigation hold procedures.
- c) Employees should see the MIEMSS Information Security Officer for disposal details and questions.

**10) Acceptable Use of State IT Resources**

- a) State IT resources are intended for business purposes in serving the interests of the State and the citizens, visitors, and commerce partners of the State of Maryland. All electronic communications created, received, or stored on the State's electronic communications systems are the sole property of the State and **not** the author, recipient, or user unless designated otherwise or protected by prevailing Federal or State law.
- b) The following activities are examples of acceptable use of agency IT Resources:
  - i) Sending and receiving electronic mail for job related messages, including reports, spreadsheets, maps etc.
  - ii) Using electronic mailing lists and file transfers to expedite official communications within and among State agencies, as well as other job related entities.
  - iii) Accessing on-line information sources to gather information and knowledge of state and federal legislation, industry best practices, or to obtain specialized information useful to state agencies.
  - iv) Connecting with other computer systems to execute job related computer applications, as well as exchange and access datasets.
  - v) Communicating with vendors to resolve technical problems.

**11) Personal Use of State Resources**

- a) Restricted Personal Use
  - i) The agency's IT Resources may be used for limited, minor, incidental personal uses, as determined by the employee's immediate supervisor and are not intentional misuses.
- b) Personal use is **not** allowed if:
  - i) The use directly or indirectly interferes with the Agency's business activities, another user's duties, or burdens the State with more than a negligible cost;
  - ii) The use violates any provision of this policy, any supplemental policy adopted by MIEMSS regarding information security and use, electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law; **or**
  - iii) The employee's immediate supervisor determines that the employee's personal use exceeds the allowance for minor, incidental, limited use or is otherwise inappropriate.
- c) For additional guidelines on acceptable and prohibited use of agency IT resources see MIEMSS Email and Internet Usage policy 137.04.

	<b>Maryland Institute for Emergency Medical Services Systems</b>		
	<i>Policy: Information Security Policy</i>		
	<i>Originator: Information Technology</i>		
	Policy Number	Effective Date	Revision Date
137.08	November 7, 2016	December 21, 2018	

**12) User Access Termination**

- a) User access will be terminated for the following reasons:
  - i) Termination of employment or consultant’s relationship with the State;
  - ii) Lay-off; or
  - iii) A determination by management that an employee's or consultant’s access may constitute a threat to the MIEMSS network or data infrastructure.

**13) Reporting Suspected/Actual Security Incidents**

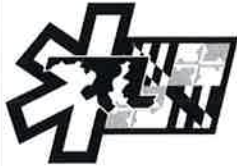
An information systems security incident is any event, suspected event, or discovery of a threat or vulnerability that could compromise the confidentiality, integrity, or availability of systems, applications, or information. An employee must immediately upon discovery report such a concern to their supervisor or management and the MIEMSS Department of Information Technology Helpdesk at [computersupport@miemss.org](mailto:computersupport@miemss.org).

**14) Sanctions for Policy Violation**

- a) MIEMSS employees must, upon employment and annually thereafter, sign the “User Information Security Policy Acknowledgement Form” attesting that the employee will follow applicable State and agency IT security policies.
- b) Any employee found to have violated these policies may be subject to disciplinary action up to and including termination of employment.
- c) Deliberate, unauthorized disclosure of PHI and PII may expose the agency and employee to substantial civil and/or criminal penalties.

**15) Required Training**

- a) The Maryland Department of Information Technology and MIEMSS have coordinated efforts in providing Information Security Awareness training. Each MIEMSS employee is required to complete training activities in accordance with state and agency requirements.
- b) All MIEMSS employees who use agency IT resources or have access to PHI and PII must complete these monitored training activities.
- c) Training Program
  - i) MIEMSS provides monthly training on information security and privacy. Training is typically provided via web-based resources. However, custom group and/or individual training sessions may be utilized as needed.
    - (1) Employees will receive notification of web-based training by email.
    - (2) Web-based training module must be completed within approximately 1 month of assignment. Required completion dates are provided at the time of training assignment.
    - (3) After the completion date, the module will be closed and no longer available.



**Maryland Institute for Emergency Medical Services Systems**

**Policy: Information Security Policy**

**Originator: Information Technology**

Policy Number	Effective Date	Revision Date
137.08	November 7, 2016	December 21, 2018

- (4) Managers will be notified by email 5 days prior to a module closing if an employee has not completed the assigned training.
  - ii) Failure to complete all assigned training may be reflected on an employee’s Performance Planning and Evaluation Program documentation (PEP).
  - iii) Managers are responsible for holding their employees accountable and ensuring compliance.
  - iv) Managers may request compliance reports form the MIEMSS IT Security Officer.
- d) Employees not receiving MIEMSS provided training, such as those working in this Emergency Response System (ERS), will be registered to receive security training provided by with the Maryland Department of Information Technology (DoIT).
  - i) The same training completion requirements outlined above shall apply.

**16) Technical Guidance / Additional Information**

Persons with questions or needing further information are encouraged to contact the MIEMSS Information Security Officer.

**17) References**

Maryland Senate Bill 553 – State Government – Security Training – Protection of Security – Sensitive Data, <http://mgaleg.maryland.gov/2018rs/bills/sb/sb0553f.pdf>

**Public/Private Designation: Public** - This document is approved for publication and unrestricted distribution.

Policy approved by MIEMSS:

Signature:   
 Patricia Gainer, JD, MPA  
 Acting Executive Director

Date: 1-19-19