	Maryland Institute for Emergency Medical Services Systems		
	Policy: Information Security – Termination of Employment		
	Originator: Information Technology		
	Policy Number	Effective Date	Revision Date
	137.01	April 18, 2011	n/a

Purpose: MIEMSS employees are responsible for safeguarding valuable data which is confidential under State and federal law, and they are provided state of the art technological equipment in order to perform their work. In order to safeguard data and to preserve State equipment upon termination of employment, it is incumbent upon MIEMSS employees to comply with the following policy.

1. An employee terminating employment shall during normal business hours prior to or on the effective date of termination:

    a. Turn in all MIEMSS purchased/issued IT equipment – desktop, laptops, USB devices, LCD projectors, and application media and activation keys, and the like.

    b. Turn in all MIEMSS purchased/issued communications equipment – cell phones, smart phones (iPhone, Blackberry, etc.), portable radios, mobile radios, paging/notification devices, commercial wireless equipment and the like.

        i. Under certain circumstances, an employee may transfer a MIEMSS cell phone number to a personal account or other employer account with written permission from the Chief of IT and Communications or designee in concurrence with the employee's department head.

    c. Turn over all passwords to all MIEMSS IT and Communications purchased/issued applications, equipment, peripherals, and accessories.

    d. Relinquish access to MIEMSS email and network.

        i. To the benefit of MIEMSS, an employee may extend email and network access beyond the employee's termination date with written permission from the Chief of IT and Communications, and the Executive Director in concurrence with the employee's department head.

    e. Relinquish access to MIEMSS applications and data. An employee may not copy and/or take and/or keep any MIEMSS data or applications.

        i. To the benefit of MIEMSS, exceptions may be granted in writing by the Chief of IT and Communications, and the Executive Director in concurrence with the employee's department head.

2. At the time of termination or announcement of intent to terminate employment with MIEMSS, an employee shall not delete any data, files and/or applications, (either MIEMSS or personal), from any MIEMSS communications or computer equipment, peripherals, or accessories without written permission from Chief of IT and Communications or designee.

Unauthorized deletion of data, files and/or applications shall be considered destruction of property and may result in an appropriate amount to cover such loss or the recovery of such data from the employee's final paycheck being withheld as well as the pursuit of other legal remedy for recovery of damages. An employee may request authorization to delete data, files and/or applications that are personal in nature by submitting a written request via the appropriate chain of command to the Chief of IT and Communications or designee.

3. Each MIEMSS employee shall be required to read and acknowledge this policy by signing a copy which shall be placed in the employee's personnel file. See Attachment A.

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

Policy approved by MIEMSS:

Date: 4/25/11

Signature: _____
Robert R. Bass, MD
Executive Director

State of Maryland

Maryland Institute for Emergency Medical Services Systems

653 West Pratt Street
Baltimore, Maryland
21201-1536

Martin O'Malley
Governor

Donald L. DeVries, Jr., Esq.
Chairman
Emergency Medical Services Board

Robert R. Bass, MD
Executive Director
410-706-5074
FAX 410-706-4768

_____ __, 20___

To all MIEMSS staff,

Information security continues to be a high priority here at MIEMSS. We must assure the confidentiality, integrity and availability of the information we collect. This is an ethical and legal responsibility borne by each of us. Accomplishing this objective requires constant vigilance. The attached policy, "Information Security – Termination of Employment," supports this objective.

The attached policy must be reviewed by all MIEMSS employees. To assure each employee has been presented with an opportunity to review the policy we are requiring each employee sign this memo and return it to their supervisor. The signed memo will be placed in your employee file.

Thanks,

Robert R. Bass, MD
Executive Director

I, _____, have read and understand the attached policy,
(Print your name here.)
effective on _____ __, 20__, "Information Security – Employment Termination."

_____ _____
Employee Signature Date Signed

_____
Witness