



NUMBER: 7.3.01

DATE: 02/02/2002

REVISION: 11/06/2008; 2/28/2011

PAGE: 1 of 5

SECTION: INFORMATION TECHNOLOGY

AREA: NETWORK SECURITY

SUBJECT: IT SECURITY INCIDENT IDENTIFICATION & HANDLING POLICY

## PURPOSE

To protect the integrity, availability and confidentiality of Confidential Information including ePHI, to prevent loss of service, and to comply with legal requirements.

## SCOPE

UAMS workforce

## DEFINITIONS

**UAMS Workforce** means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

**IT Security Incident** is any activity that harms or represents a threat to the whole or part of UAMS's computer and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, software or data, unauthorized exposure, change or deletion of ePHI or non-public personal information, or a crime or natural disaster that destroys access to or control of these resources. IT Security Incident includes the loss of ePHI or non-public personal information through the theft or loss of a mobile device, including laptop computer, PDA or Smartphone, and USB flash drive.

To access any other terms or definitions referenced in this policy:

<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

## POLICY

Each user of the UAMS computing systems has a responsibility to report IT Security Incidents or violations of UAMS IT Security policies. All Security Incidents will be reported to the IT Security Team as soon as an incident comes to the attention of the user. The IT Security Team will oversee the Security Incident handling in accordance with the procedures set forth below.

## PROCEDURES

### **A. Security Incidents – Intrusions or Vulnerabilities**

Any IT Security Incident should be immediately reported to the IT Security at (501) 686-8555.

IT Technical Security shall perform scans of the UAMS network to test for and identify any potential vulnerability (virus, external intrusion or hacker attack, broadcast storm, etc.) present on workstations, servers, and other networked devices, taking into consideration the operational functions and number of end users affected.

1) If a potential vulnerability is identified, IT Technical Security shall notify the appropriate person(s) via phone and/or email. Depending upon the nature and severity of the incident a follow-up to the event may be performed.

2) Any incident identified as having taken place on the UAMS campus shall be classified as one of the following severity levels:

- **Level 1 (Critical):** Machine is infected, compromised, or a high-risk vulnerability is detected  
**Action:** Device will be removed from the network and repaired (see below)
- **Level 2 (Warning):** Medium risk vulnerability detected  
**Action:** Device must be corrected or disconnected from the network within 72-hours
- **Level 3 (Information):** Low risk vulnerability detected  
**Action:** Notification only, updates are optional

3) If a Level 1 incident occurs on the UAMS network:

- All identified LAN Administrators or backup personnel will be informed of the incident.
- The UAMS Technical Support Center (TSC) will be informed of the incident and advised as to its impact upon personnel and equipment attached to the UAMS network. The TSC shall also be instructed on what steps to take and how to inform users to lessen the impact of the incident.
- If the incident could potentially involve ePHI, the UAMS HIPAA Campus Coordinator will be notified immediately and an Incident Response Committee will be established as an advisory committee to the UAMS HIPAA Campus Coordinator. The Incident Response Committee will include, as necessary, key representatives of UAMS IT, administrators of affected schools and hospital, Campus Police, General Counsel, and Public Affairs.

4) Network, workstations, servers, and/or networked devices may be removed from the network, if required to protect the integrity of the network, until the threat has been removed from the device. Under no circumstances shall the device be reconnected until the threat has been eliminated unless reconnection is approved by the UAMS CTO or the UAMS CIO. Any personally-owned devices, such as PDAs, phones, wireless devices or other electronic transmitters which have been used to store ePHI or non-public personal information and are determined to contribute to an Incident, may be subject to seizure and retention by UAMS until the IT Security Incident has been remediated, unless the custody of these devices is required as evidence for a court case.

- 5) If required by law, appropriate local, state, and federal law enforcement agencies, as well as regulatory agencies and oversight agencies, may be notified of the incident, and the appropriate logs and notes turned over to them for further investigation of the incident. It will be the decision of the UAMS HIPAA Campus Coordinator, with the advice of the Incident Response Committee, to notify law enforcement and/or regulatory and oversight agencies.
- 6) If required by law, individuals affected by the IT Security Incident will be notified. The HIPAA Campus Coordinator, with the advice of the Incident Response Committee, will determine whether notification is required for incidents involving ePHI, and will coordinate notification of affected individuals. For notification of individuals other than when ePHI is involved, the system custodian shall be responsible for notification.
- 7) All communications with the media regarding the incident will require coordination with the HIPAA Campus Coordinator, who will consult with the Incident Response Committee.
- 8) When applicable, other organizations and entities outside of UAMS shall be notified to take appropriate precautionary or remedial steps.
- 9) All IT individuals involved with the incident shall keep a log from start to finish of their own activities involved in remedying the situation. These notes shall be audited and filed by IT Security and all network related incidents will be reviewed with the IT Coordinating Committee. All potential evidence related to the security incident and all security incident reports will be retained by IT Security for a minimum of six years for those incidents involving PHI and one year for all others.

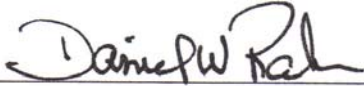
## **B. Security Incidents – By Request**

- 1) Security incidents may be implemented by request from management to resolve or collect evidence of employee non-compliance with UAMS, state, local, or Federal policies and laws. Such request is made by properly completing the Security Incident Request Form in section D below. Division level approval is required before any action is taken by IT Security to monitor, collect or report on any employee's internet usage, local profile, or email. Email reporting requires completion of an additional form, located in policy [7.1.12 Email Access and Usage](#).
- 2) Network bandwidth monitoring is an exception to the general procedure above. The bandwidth usage at UAMS will be monitored by IT Network Security through the use of an automated process that creates a top twenty (20) list of high usage workstations. Workstations on this list are reviewed daily to verify the legitimacy of the high bandwidth usage in relation to appropriate UAMS business use. When the high bandwidth usage is found to be non-compliant a report including the user information is made to the CIO who distributes it to the proper Division level officer for dispersal to

lower management to use in employee discipline. The primary purpose of this procedure is to ensure that there is enough bandwidth for mission critical applications at UAMS.

### **C. Sanction**

Violation of this policy will result in disciplinary action as set forth in the [Employee Disciplinary Notice Policy #4.4.02](#).

Signature: 

Date: May 11, 2011

