UNM HEALTH SCIENCES CENTER

Applies To: **HSC**
Responsible Office**: HSC Information Security Office**
Effective:12/22/2011

Title: **HSC-240 IT Security Incident Response**	**Policy**

Responsible Authority **Last Revision: New Policy**
Chancellor for Health Sciences
HSC Executive Compliance Committee with advice from the IT Security Council
HSC Information Security Officer (ISO) / HIPAA Security Officer

Policy Sections ……page

SCOPE

This policy governs the HSC general response, documentation, reporting and escalation of IT Security incidents affecting computerized data and electronic communication information resources, such as theft, intrusion, misuse of data, compliance violations, denial of service, corruption of software, other activities contrary to the University's Acceptable Use Policy and incidents reported to the HSC by other institutions and business entities.

UNM Health Sciences Center policies apply to all health care components of UNM that are under the jurisdiction of the HSC as designated in UNM Board of Regents Policy 3.4 Subject: Health Sciences Center and Services and UNM Board of Regents Policy 3.7 Subject: Institutional Compliance Program.

POLICY STATEMENT

The HSC IT Security Incident Response Policy and subordinate procedures define standard methods for detection and analysis, containment, eradication/mitigation, recovery and post-incident review of network and computer-based IT Security incidents/events. This policy will differentiate between incidents that occur as part of normal operations, and Emergency or Significant/Major incidents which will be escalated to the HSC Incident Management Team (IMT).

REASON FOR POLICY

The HSC IT Security Incident Response Policy is established to protect the integrity, availability and confidentiality of Confidential or Restricted information, including ePHI, to prevent loss of service and to comply with regulatory requirements. This policy establishes the coordination of the HSC response to computerized and electronic communication systems incidents to enable timely remediation, information gathering and reporting of security related events.

DEFINITIONS

Refer to the HSC Master Glossary of IT Security Terms.

POLICY SECTIONS

HSC-240.1 Incident Identification and Reporting

An Incident, as defined in HSC-200, is "Any adverse event whereby some aspect of UNM/HSC computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. A security incident may be logical, physical or organizational, for example a computer intrusion, loss of secrecy, information theft, fire or an alarm that doesn't work properly, and may be accidental or deliberate."

An Emergency or Significant/Major Incident is defined as an incident involving a significant amount of Confidential Level 1 data (Reference: HSC-210), a critical system, or a significant number of non-critical systems. These incidents will be referred to the HSC IMT by the HSC ISO or appropriate System Owner for a coordinated response.

Any member of the HSC community, or individual or organization outside of the HSC, may refer an activity or concern to the HSC ISO directly or through their supervisor and/or support services. IT staff can also identify an incident through proactive monitoring of HSC network and information system activities, as authorized. Once identified, the HSC ISO will use standard internal procedures to document and track incidents and, working with others as appropriate, take steps to investigate, escalate, and remediate. The HSC ISO may refer an incident which becomes an emergency or involves multiple systems and/or Confidential (Level 1) information as outlined in policy HSC-210 to the HSC IMT for review and/or action, including the creation of a formal Security Incident Response Team (SIRT) as described below.

HSC-240.2 Event Classification and Risk Assessment

The HSC ISO maintains an internal risk assessment classification to focus the response to each system and event classification. This classification corresponds to an escalation of contacts across the HSC, and indicates which authorities at the HSC to involve and which procedures would be applicable for each class of event. Initial event investigation will be handled by a local incident response team comprised of component IT Security staff; other participants may be added by the HSC ISO, HSC IMT or other appropriate body or bodies. If an event is escalated to an Emergency or Significant/Major Incident status, a formal Security Incident Response Team (SIRT) will be created according to the details in the remainder of this policy and associated procedures. Communication between the local incident response team or the SIRT (as appropriate based on the incident classification) and HSC Management, System Owners, and the HSC IMT will be coordinated by the HSC ISO.

HSC-240.3 Security Incident Response Team (SIRT) Creation

This section outlines the basic starting process of the SIRT; procedures associated with this policy should be referenced for specific details. The purpose of the Security Incident Response Team is incident interdiction and remediation of Emergency or Significant/Major IT security events that affect the confidentiality, integrity or availability of HSC electronic information assets. Any such event will be escalated to the HSC Chancellor or his delegate to

address the creation of a formal SIRT. The SIRT will operate under the direction of the HSC Incident Management Team (IMT) or the Chair of the IT Security Council.

HSC-240.4 Communication and Documentation
The HSC ISO will work to maintain appropriate incident documentation and archives. Incident reporting will be provided by the HSC ISO to the HSC Compliance Office and IT Security Council.

The HSC ISO and/or the SIRT representatives will be responsible for: initiating and maintaining confidential communications regarding the incident to appropriate personnel; maintaining contact for the purposes of updating and instruction; or referral for escalation to the HSC IMT. The HSC ISO will be responsible for communication and coordination between the HSC IMT and the SIRT team until the Emergency or Significant/Major Incident has been closed.

HSC-240.5 Incident Eradication/Mitigation and Recovery
To limit potential damage to IT resources and maintain critical HSC services the local incident response team and/or the SIRT will take responsibility for eradication, mitigation and recovery as needed while at the same time ensuring the preservation of evidence. The HSC ISO will work with the SIRT, HSC IMT, the affected System Owners, and local department administration to coordinate a timely response and allocation of resources needed to implement the mitigation and recovery strategy.

HSC-240.6 Emergency Operations Center, Federal and State Relationships
A response plan or remediation initiated pursuant to this policy may be integrated with or preempted as required by the Emergency Operations Center, and/or federal or state officials. The HSC may also permit integration or preemption at the discretion of the Chancellor.

PROCEDURES

The HSC ISO maintains internal procedures for incident documentation, tracking and reporting, for evidence custody and related practices.

HSC-240 PR.1 Incident Response Team Procedures and Guidelines

HSC-240 PR.2 Security Incident Response Team (SIRT) Procedures and Guidelines

RELATED INFORMATION

HSC Policy HSC-200 Security and Management of HSC IT Resources
HSC Policy HSC-210 Security of HSC Electronic Information
HSC Policy HSC-220 Information Access and Security
HSC Policy HSC-230 Electronic Data Storage and Transmission
HSC Policy HSC-250 Systems and Network Security
HSC Policy HSC-260 Device and Media Control
HSC Policy HSC-270 Information Systems Activity Review

HSC Policy HSC-280 Physical Security
HSC Policy HSC-300 ePHI Security Compliance

RETIRED POLICIES SUPERSEDED BY THIS POLICY

HSC Policy 8.1 Security Incident Procedure - ePHI
HSC Policy 8.2 Response and Reporting - ePHI

CONTACTS

Subject	Contact	Phone
IT Security Policy Matters	HSC Information Security Officer	505-272-1696
HIPAA Privacy Matters	HIPAA Privacy Officer	505-272-1493

DOCUMENT APPROVAL & TRACKING

Item	Contact	Date	Approval
Owner	Barney D. Metzner, HSC ISO, HIPAA Security Officer 272-1696		
Committee(s)	HSC Executive Compliance Committee, HSC IT Security Council		Y
Legal (Required)	Scot Sauder, Senior Associate University Counsel-- Health Law Section Leader, Office of University Counsel		Y
Official Approver	Dr. Paul Roth, Chancellor for Health Sciences		
Official Signature		Date: 12/22/2011	
Effective Date:		12/22/2011	
Origination Date:		4/2011	
Issue Date:		1/9/2012	ar

ATTACHMENTS

None.