UNM HEALTH SCIENCES CENTER

Applies To: **HSC**
Responsible Office**: HSC Information Security Office**
Revised: New 12/2010

Title: **HSC-200 Security and Management of HSC IT Resources**	**Policy**

POLICY STATEMENT

The University of New Mexico Health Sciences Center (HSC) expects all individuals using information technology devices that at any time connect to the HSC network to take appropriate measures to manage the security of those devices.

DETAILED POLICY STATEMENT

The university must preserve its information technology resources, comply with applicable Federal regulations (HIPAA, FERPA, etc.) and state legislation, and maintain good security practices as a matter of public trust and confidence. Toward these ends, faculty, staff, students, and other HSC community members must share in the responsibility for the security of information technology devices.

APPLICABILITY

All units of the UNM Health Science Center. All UNM workforce members who have access to HSC information systems containing administrative, research, student and patient information. Additionally, all healthcare components of UNM that are under the jurisdiction of HSC as designated in UNM Board of Regents Policy Number 2.13.4 – University HIPAA Compliance Policy.

WHO SHOULD READ THIS POLICY

All members of the UNM Health Sciences Center community.
All UNM workforce members who have access to HSC information systems containing administrative, research, student and/or patient information.

POLICY AUTHORITY

Executive Vice President for Health Sciences
HSC Executive Compliance Committee with advice from the IT Security Council
HSC Information Security Officer (ISO) / HIPAA Security Officer

RELATED DOCUMENTS

UNM/HSC Documents
- UNM Business Policies and Procedures Manual
- UNM Faculty Handbook
- UNMH Administration and Human Resources Policies
- HSC Compliance and HIPAA Policies
- Security of HSC Electronic Information
- HSC Unit IT Security Guidelines
- Current Policies:
  1. HSC Policy 8.1, Security Incident Procedure
  2. HSC Policy 8.2, Response and Reporting
  3. HSC Policy 4.5, Information Access Authorization, Establishment, and

Modification
4. HSC Policy 2.1, Security Management Process
5. HSC Policy 7.1, Workstation Use and Security

UNM/HSC Training

HSC Code of Conduct; HSC Culture of Compliance

HSC HIPAA Competencies; HIPAA and Breach Notification

Other Documents:

Health Insurance Portability and Accountability Act

DEFINITIONS

The following definitions apply to these terms as they are used in this policy.

Information Technology (IT) Security Incident	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.
Information Technology (IT) Device	Any device involved with the processing, storage, or forwarding of information making use of the UNM/HSC (IT Device) information technology infrastructure or attached to the HSC network. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, smartphones, servers, network devices such as routers or switches, printers, and devices that serve a clinical function.
Information Technology (IT) Resources	The full set of information technology devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, and transmission of information.
Local Support Provider	An individual (either assigned by central IT support or a member of the unit) with responsibility for local IT device support. These individuals are responsible for meeting HSC IT device standards by following HSC practices with regard to the installation, configuration, security, and ongoing maintenance of an information technology device.
Software Patch	Software that is distributed to fix a specific set of problems or vulnerabilities in such things as computer programs or operating systems. A computer vendor will usually distribute a patch as a replacement for or an insertion in compiled code within computer operating systems or applications.
Unit	An HSC department, program, research center, business service center, or other operating unit.
Unit Head	The individual with administrative responsibility for a unit.
Unit Security Liaison	The person whom the Unit Head designates as the primary contact for the HSC Information Security Officer.
User	Any individual who uses an information technology device such as a computer.
HSC Information Security Officer	The HSC Information Security Officer is the university officer with the authority to coordinate HSC campus information technology security, with a specific focus on Confidential (Level 1) information described in the HIPAA Security Rule. The HSC ISO reports to the IT Security

	Council and Executive Compliance Committee. Through direction from those committees and through consultation with KMIT Committees and other stakeholders, the HSC ISO determines technical, administrative, and physical IT security procedures and reviews them annually, at a minimum.
Malware (virus)	Shortened form of the term "malicious software" which is software designed to infiltrate a computer system without the user's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term computer virus is sometimes used as a catch-all phrase to include all types of malware including true viruses. (Reference: Wikipedia "Malware")

OVERVIEW

Introduction

In order to manage information technology security comprehensively, this policy serves four major purposes.

1. It establishes the principle that every information technology (IT) device connected to the HSC network must have at least one individual managing the security of that device.
2. It requires units to designate Unit Security Liaisons (see the "Obligations of the Unit Security Liaison" segment of this document).
3. It creates the following five categories of individuals, each with specific obligations and responsibilities regarding the security of information technology devices:
   - User;
   - Local Support Provider;
   - Unit Security Liaison;
   - Unit Head;
   - HSC Information Security Officer (HSC ISO).
4. The HSC ISO can modify obligations by submitting additions/modifications for approval by the IT Security Council which would, upon acceptance, submit the changes to the Executive Compliance Committee or the Executive Vice President for Health Sciences for final approval.

Note: All users of IT devices must follow the procedures outlined in the "Obligations of Users" segment of this document.

Note: The focus of this policy is on the security of information technology devices and resources, and not on specifics for the management of data or any particular class of data. For information concerning data, please consult the following:
(1) Policy HSC-210 Security of HSC Electronic Information, which provides the authority for and guidance toward maintenance and protection of institutional information assets and compliance with applicable Federal regulations (HIPAA, FERPA, etc.) and state legislation, and
(2) HSC Policy 2.1, Security Management Process, which provides the

	authority for and guidance toward the development of procedures for the access to, as well as the preservation and proper management of, data in specific functional areas.

PROCEDURES

Obligations of the User	Any individual who uses an IT device (see the "Definitions" section of this document) is a user. Each of these devices may or may not have a Local Support Provider assigned to it. Typically, HSC-owned IT devices located in campus workspaces have Local Support Providers assigned to them. **Note:** If you cannot perform or do not understand any of the obligations assigned to users, contact the HSC Support Centers, UNMH at UHHelpDesk@salud.unm.edu or HSLIC at Helpdesk@salud.unm.edu **Obligations of a User** 1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the HSC's electronic networks and devices (see the "Related Documents" section of this document). 2. Comply with guidelines and practices established by the Local Support Provider for the IT device. 3. Contact your Local Support Provider or Unit Security Liaison whenever a questionable situation arises regarding the security of your IT device. 4. If there is no Local Support Provider, contact the Unit Security Liaison to determine the appropriate HSC Support Center which will install and maintain HSC-approved security applications (anti-virus, operating system updates, application updates, etc.). 5. Protect the resources under your control with the responsible use of secure passwords. Contact your Local Support Provider or Unit Security Liaison with any questions. 6. Under the direction of the Local Support Provider or appropriate HSC Support Center, assist as requested to remediate a detected vulnerability or compromise. 7. Comply with directives of HSC officials such as the HSC Information Security Officer, as well as the Unit Security Liaison, or Local Support Provider(s), to maintain the security of devices attached to the network. 8. Follow IT security incident reporting requirements in accordance with HSC Policy 8.1, Security Incident Procedure.
Obligations of a Local Support Provider	A Local Support Provider is an individual (either assigned by central IT support or a member of the unit) with responsibility for local IT device support. These individuals are responsible for meeting HSC IT device standards by following HSC practices with regard to the installation, configuration, security, and ongoing maintenance of an IT device. A Local

	Support Provider seeking guidance or clarification should contact his or her Unit Security Liaison or the HSC Information Security Officer. The Local Support Provider will be knowledgeable and comply with the current policies, requirements, guidelines, procedures and protocols concerning the security of the HSC's information technology resources as defined by this policy and the HSC ISO. 1. Follow the HSC Policy, Security of HSC Electronic Information for configuring and securing IT devices. 2. Understand and document the specific configurations and characteristics of the IT devices he or she supports to be able to respond to emerging information technology threats and to support security event mitigation efforts appropriately. 3. Understand and recommend the appropriate measures to provide security to the resources under his or her unit, including physical, administrative, and technical security as determined by the HSC ISO. 4. Follow IT security incident reporting requirements in accordance with HSC Policy 8.1, Security Incident Procedure. **Note:** Local Support Providers should be mindful of potential responsibilities they may have as custodians of unit data transmitted or stored on IT devices under their control. Please consult HSC Policy, Security of HSC Electronic Information, for further guidance.
Obligations of the Unit Security Liaison	The Unit Security Liaison is the person whom the Unit Head designates as the primary contact for the HSC Information Security Officer. For further guidance or clarification, contact the HSC ISO. The Unit Security Liaison is responsible for the following: 1. Act as the unit point of contact with the HSC ISO. 2. Implement a security program consistent with the requirements of this policy (for example, the implementation of security assessment, best practices, education and training), consistent with HSC Policy, Security of Electronic Information and in keeping with the specific information technology security needs of his or her unit. This will include the following: a. Identify the information technology resources within his or her unit. b. Provide proper information and documentation about those resources. c. Oversee compliance with applicable Federal regulations (HIPAA, FERPA, etc.) and state legislation. d. Respond to, coordinate, and support security risk assessments for the unit's information technology resources. 3. Implement unit procedures and protocols for the reporting of IT security incidents in accordance with HSC Policy 8.1, Security Incident Procedure. **Note:** The Unit Security Liaison may want to take specific measures

	toward the protection of data stored or transmitted on the IT devices for the unit and/or be mindful of any potential responsibilities as custodians of unit data. Please consult with HSC Policy, Security of HSC Electronic Information for guidance.
Obligations of the Unit Head	Unit Heads have overall, local responsibility for the security of information technology resources under their control. For further guidance, contact the HSC Information Security Officer. The Unit Head's oversight responsibilities in relation to security information technology resources include, but are not limited to, the following: 1. Identify a Unit Security Liaison to the HSC Information Security Officer. The Unit Security Liaison may also be the Local Support Provider (depending upon the size of the unit). 2. Ensure that, through the Unit Security Liaison, a security program is implemented for the unit consistent with requirements of this policy (for example, the implementation of security assessment, best practices, education and training). The security program must follow HSC Policy, Security of HSC Electronic Information, as well as address the specific information technology security needs of his or her unit. 3. Control continuity of support for all the IT devices in the unit such that termination or a change in the role of the Local Support Provider will not result in the abandonment of responsibility for those IT devices. 4. Oversee the creation and implementation of procedures for the reporting of IT security incidents in accordance with HSC Policy 8.1, Security Incident Procedure. **Note:** Unit Heads may want to take specific measures toward the protection of data stored or transmitted on the IT devices under their management. Please consult HSC Policy 2.1, Security Management Process and HSC Policy, Security of HSC Electronic Information for guidance.
Obligations of the HSC Information Security Officer	The HSC Information Security Officer is the university officer with the authority to coordinate HSC campus information technology security, with a specific focus on Confidential (Level 1) information described in the HIPAA Security Rule. The obligations of the HSC Information Security Officer are to: 1. Develop a comprehensive security program that includes risk assessment, best practices, education, and training. 2. Assist or lead IT security incident resolution for the HSC and individual units. 3. Strive for proper identification, analysis, resolution, and reporting of HSC IT security incidents. 4. Develop, implement, and support HSC-level security monitoring and analysis. 5. Support and verify compliance with applicable Federal regulations

	(HIPAA, FERPA, etc.) and state legislation.

SUMMARY OF CHANGES

New Policy

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, Executive Vice President for Health Sciences		
Official Signature		Date: 12/21/2010	
Effective Date:		12/21/2010	
Origination Date:		12/2010	
Issue Date		1/7/2011 ar	

ATTACHMENTS

None.