

## **OVERVIEW**

The University of New Mexico Health Sciences Center (HSC) expects all institutional information stewards and custodians who have access to and responsibilities for electronic HSC administrative, research, student and patient information to manage it according to the rules regarding storage, disclosure, access, classification of information and minimum privacy and security standards as set forth in the HSC policy Security of HSC Electronic Information.

This standard operating procedures document defines baseline IT security requirement for securing a computing device used for HSC business whether located on HSC owned premises or elsewhere. The procedures are strongly recommended for all computing devices whether connected to a network or not. For some uses, the procedures are mandatory. The methods actually used to implement the procedures as well as additional, more stringent, procedures will vary with specific location and will be detailed by the Unit Head, Unit Security Liaison, and/or Local Support Providers.

## **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 stewards and custodians of electronic HSC administrative, research, student and patient information.

## **DOCUMENT 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**

HSC Policy, Security of HSC Electronic Information

**BASELINE IT SECURITY REQUIREMENTS FOR ALL COMPUTERS**

<p><b>Requirements for All Computers</b></p>	<ol style="list-style-type: none"> <li>1. Keep all relevant operating system, server and application software up to date. <ul style="list-style-type: none"> <li>✓ A defined patch management process must ensure that all security/critical updates are installed without undue delay.</li> <li>✓ Any use of operating systems and/or applications no longer supported by the vendor must be approved as an exception by the HSC ISO.</li> </ul> </li> <li>2. Configure user privileges to be as low as possible while still meeting business needs. Consistent or regular use of the administrator or root account is discouraged.</li> <li>3. Unit Security Liaisons must maintain an inventory of all applications in use by the unit for licensing purposes.</li> <li>4. HSC NetIDs and passwords must not be used outside of the HSC authentication infrastructure (gmail, Facebook, etc.)</li> <li>5. Ensure all other HSC accounts have strong passwords at least equivalent to the strength required for NetID passwords. <ul style="list-style-type: none"> <li>✓ All electronic distribution of passwords must be encrypted.</li> </ul> </li> <li>6. All passwords should be regularly changed as defined by UNM/HSC standards.</li> <li>7. For any computer system, not in a secure private space accessing Confidential (Level 1) or Restricted (Level 2) data, specific requirements for logon/logoff and screen locking are defined in HSC Policy 4.5, Information Access Authorization, Establishment, and Modification.</li> <li>8. Ensure local/personal firewalls (Windows Firewall, MacOS X firewall, McAfee Anti-virus Firewall, etc.) and/or IPSec filters are installed and running.</li> <li>9. On all Windows and Macintosh systems, run centrally-monitored anti-malware software with daily updates and active protection enabled. Solutions other than the HSC standard, currently McAfee Total Protection Suite, should be noted on the exception report and must provide equivalent protection and reporting capabilities. <ul style="list-style-type: none"> <li><input type="checkbox"/> Suggestion: Run an anti-malware package on Linux systems, as well.</li> </ul> </li> </ol>
<p><b>Requirements Specific to Desktops and Laptops</b></p>	<p><b>Individuals are allowed to access Confidential (Level 1) and/or Restricted (Level 2) information remotely, subject to (1) the receipt of proper authorization, and (2) adherence to the procedures contained in HSC Policy 7.1, Workstation Use and Security.</b></p> <p><b>The storage of Confidential (Level 1) and/or Restricted (Level 2) information on remote devices is subject to all requirements set out in this policy, Security of HSC Electronic Information.</b></p> <ol style="list-style-type: none"> <li>1. All local shares and other mechanisms for file access must be password protected. <ul style="list-style-type: none"> <li>✓ This item forbids “open shares” (unauthenticated read/write</li> </ul> </li> </ol>

	<p>access), “drop folders” (unauthenticated write-only access) and “public folders” (unauthenticated read-only access) on an individual’s system.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Suggestion: Use approved network file storage instead of local shares.</li> </ul> <p>2. If multiple individuals use a system, each should have his or her own login account, or the system should be restored to a known, clean state prior to each individual use. This also applies to “loaner” systems.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Suggestion: The account used for daily operations must be configured to not allow software installs, or must require the account password for any software installations.</li> <li><input type="checkbox"/> Suggestion: Where feasible, consider not giving end users any accounts that permit software installation.</li> </ul> <p>3. Desktop systems are not allowed to store unencrypted Confidential (Level 1) information on local devices except under the following conditions:</p> <ul style="list-style-type: none"> <li>1) The Unit Security Liaison provides an alternate solution to secure the information, subject to the following: <ul style="list-style-type: none"> <li>(a) Local solutions must be reviewed and approved by the HSC ISO prior to use. Any exceptions are subject to review by the ITSC and the ECC.</li> <li>(b) The Unit Security Liaison will maintain a list of all IT resources that require an exception, and review them on an annual basis.</li> <li>(c) Use of a unique password, not shared with other systems, for local administrator accounts (accounts with elevated privileges). <ul style="list-style-type: none"> <li>✓ In particular, the local administrator password used by IT support staff must be different for each system that holds Confidential (Level 1) information. Passwords must meet existing HSC password standards.</li> </ul> </li> </ul> </li> </ul> <p>4. Confidential (Level 1) information stored locally on a system, even if encrypted, must be removed when no longer needed on an operational basis.</p> <ul style="list-style-type: none"> <li>✓ Every six months, use Spider or an equivalent application to identify unencrypted Confidential (Level 1) information stored on local system drives.</li> <li><input type="checkbox"/> Suggestion: No storage of Confidential (Level 1) information on individual staff machines.</li> </ul> <p>5. Confidential (Level 1) information must be encrypted on the following:</p> <ul style="list-style-type: none"> <li>(a) Any system that, even on a temporary basis, is not located on one of the HSC campuses or some other formal HSC location; and</li> <li>(b) Any laptop or other portable device, including PDAs, smart phones and media (external hard drives, USB thumb drives, CDs,</li> </ul>
--	--

	<p>DVDs, tapes, diskettes), that ever leaves a secure location that is accessible only to authorized HSC personnel; and</p> <p>(c) Any other system that is not physically secured or in a secure location accessible only to authorized HSC personnel.</p> <ul style="list-style-type: none"> <li>• If full-volume encryption is used, the volume should be mounted only when the system is in active use. (Use the HSC centrally-managed and approved encryption solution to ensure that the encryption does not interfere with your ability to create and retrieve backups.)</li> <li>• Protect encryption keys against disclosure, misuse, and loss. See HSC Policy 4.11, Encryption and Decryption.</li> <li>• While new versions of Microsoft Office (i.e., Office 2007 and 2010) include a facility for appropriately strong encryption of documents, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications, which may or may not fulfill this requirement, require HSC ISO approval.</li> <li>• Use of the HSC standard encryption software, currently McAfee Endpoint Encryption, is required. Other solutions that may be used, if procedures are approved by the HSC ISO, include: BitLocker under Windows Vista and Server 2008, FileVault under Mac OS X, TrueCrypt.</li> </ul> <p><input type="checkbox"/> Suggestion: Encrypt all instances of Confidential (Level 1) information under the custodianship of individual staff members.</p> <p>6. Unless the Confidential (Level 1) information is protected by encryption, only authorized HSC personnel may have access to the system.</p>
<p><b>Requirements Specific to Public Workstations and Kiosks</b></p>	<ol style="list-style-type: none"> <li>1. Such systems may never be used for processing of Confidential (Level 1) information.</li> <li>2. Such systems may not be on the same subnet as computers used to conduct HSC business.</li> <li>3. Such systems must display an appropriate logon banner or bear signage with: <ul style="list-style-type: none"> <li>✓ a statement about responsible use</li> <li>✓ a warning about using the system for personal or sensitive information</li> <li>✓ a reminder to logout and/or clear any active credentials.</li> </ul> </li> <li>4. No local file shares permitted.</li> <li>5. If a user needs system privileges (ability to write files), then the computer must be restored to a known, clean state between individual sessions.</li> <li>6. Visually inspect such systems regularly, at the very least on a quarterly basis, to see if physical security has been compromised.</li> <li>7. Any exceptions must have clearly-defined procedures and be approved by the HSC ISO. <ul style="list-style-type: none"> <li>✓ This includes any individual or class of workstation configured to</li> </ul> </li> </ol>

**BASELINE IT SECURITY REQUIREMENTS FOR ALL SYSTEMS AND NETWORKS**

<p><b>Requirements Specific to Application and File Servers</b></p>	<ol style="list-style-type: none"> <li>1. Follow hardening guidelines for the operating system and any applications or services that connect to the network.               <ul style="list-style-type: none"> <li>✓ HSC practices for server builds and baseline hardening.</li> <li>✓ Along with the software vendor, credible sources for guidelines include NIST, CIS, NSA, SANS, ISO.</li> <li>✓ Disable all network services, including specific application features, that are not needed for the system to fulfill its function.</li> <li>✓ Change any passwords with default values set by the vendor.</li> </ul> </li> <li>2. Confidential (Level 1) information and information that is being made available for public access may not be on the same system.               <ul style="list-style-type: none"> <li>✓ An open Web site, i.e., one that does not require authentication for access, may not be run on a system holding Confidential (Level 1) information.</li> <li>✓ The HSC ISO must review and approve peer-to-peer (P2P) file-sharing software running on a system holding Confidential (Level 1) information.</li> <li>✓ Confidential (Level 1) information and information available for public access may reside in different virtual machines running on the same system, subject to approval by the HSC ISO. At a minimum, the host system and the host operating system must meet all the requirements for a file or application server holding Confidential (Level 1) information.</li> </ul> </li> <li>3. Activate operating system logging, and where possible application logging, with logs to be retained for at least 90 days if feasible. The following should be logged:               <ul style="list-style-type: none"> <li>✓ Access to all audit logs</li> <li>✓ Access to Confidential (Level 1) information</li> <li>✓ Failed access attempts</li> </ul> </li> <li>4. Maintain an inventory of all systems holding Confidential (Level 1) information.               <ul style="list-style-type: none"> <li>✓ On a quarterly basis, perform an inventory review to incorporate any significant changes.</li> <li>✓ File a copy of the current inventory with the local IT Unit Executive/Head and the Unit Security Liaison.</li> </ul> </li> <li>5. On at least a semi-annual basis, randomly sample accounts that grant access to Confidential (Level 1) information to verify that access is limited to authorized personnel. Any exceptions must be approved by the HSC ISO.               <ul style="list-style-type: none"> <li><input type="checkbox"/> Suggestion: Audit file, application, and system privileges on a periodic basis.</li> </ul> </li> <li>6. All application and file servers must be housed in a physically secure computer room or data center.</li> </ol>
---	--

	<ul style="list-style-type: none"> <li>✓ Entry must be logged and the logs retained for at least five days.</li> <li>☐ Suggestion: Where feasible, log exits as well.</li> <li>✓ Video monitoring is an acceptable solution to this requirement.</li> <li>✓ Visitors not permitted except under escort.</li> </ul> <p>7. An individual's access to a store of Confidential (Level 1) information should be via an account assigned by an authorized account manager for the sole use of that individual.</p> <ul style="list-style-type: none"> <li>✓ This requirement is not to be interpreted as disallowing access to an encrypted dataset via a shared encryption key.</li> </ul> <p>8. Confidential (Level 1) information should be removed from file servers when it is no longer needed on an operational basis. To the extent feasible, this also applies to Confidential (Level 1) information stored in databases and other application frameworks.</p> <p>9. Fully document all security controls and file a copy of the current documentation with the local IT Unit Executive/Head and the Unit Security Liaison.</p>
<b>Network Security</b>	<p>On at least an annual basis an assessment of the HSC network infrastructure and environment should be done that includes the following:</p> <ol style="list-style-type: none"> <li>1. Review network security mechanisms, including edge Access Control Lists, firewalls, etc.</li> <li>2. On a periodic basis, audit any VPN or other gateway accounts to ensure that only current, authorized personnel have access to internal/departmental systems.</li> <li>3. The edge ACL or other packet- and/or content-filtering mechanism on all subnets, particularly those with systems that contain Confidential (Level 1) or Restricted (Level 2) information, must employ a default-deny strategy that prohibits unnecessary inbound, internal and external connections and that strictly limits access to the systems containing such data.</li> </ol> <ul style="list-style-type: none"> <li>☐ Suggestion: Where off-campus connectivity is not needed, put the system into a non-routable space (i.e., 10 space).</li> </ul> <ol style="list-style-type: none"> <li>4. Any system holding or accessing Confidential (Level 1) information that uses a campus wireless connection must use HSC-Secure, an approved security tunnel such as VPN or SSL, or other remote access solutions approved by the HSC ISO.</li> <li>5. Any remote, off-campus access to a system containing Confidential (Level 1) information must use an encrypted communication method approved by the HSC ISO. <ul style="list-style-type: none"> <li>✓ Examples of encrypted network transport include ssh/sftp, SSL/TLS, a VPN with encryption enabled.</li> </ul> </li> <li>6. Fully document the list of services, protocols and systems permitted access into such subnets. <ul style="list-style-type: none"> <li>✓ A subnet's ACL list or firewall rule set suffices to fulfill this requirement.</li> <li>✓ Review this documentation on a semiannual basis.</li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>✓ File a copy of the current documentation with the local IT Unit Executive/Head and the Unit Security Liaison.</li> </ul> <p>7. Other systems such as content controls may be implemented as deemed necessary for security, subject to central control exceptions approved by the HSC ISO.</p>
<p><b>Security Reviews and Assessments</b></p>	<p>On at least an annual basis, based on ITSC review and authorization, assess the local infrastructure and environment. This assessment should include the following:</p> <ol style="list-style-type: none"> <li>1. Run a vulnerability scanner, such as Nessus or GFI LANguard, on all unit subnets and remediate high-risk vulnerabilities.</li> <li>2. Review all file and application servers, including vulnerability scans of Web sites, databases, etc.</li> <li>3. Select a sample set of staff computers and conduct content scans using Spider or an equivalent application to ensure that there are no improper instances of Confidential (Level 1) information.</li> </ol> <p><input type="checkbox"/> Suggestion: Run annual, or more frequent, content scans of all systems.</p> <ol style="list-style-type: none"> <li>4. Audit account distributions to ensure that only current, authorized personnel have access.</li> </ol>
<p><b>Additional Process and Documentation Requirements</b></p>	<p>The HSC Information Security Officer will provide templates and/or more specific guidelines for fulfilling items listed here.</p> <ol style="list-style-type: none"> <li>1. Define and document incident response and escalation procedures for a potential loss of Confidential (Level 1) information. <ul style="list-style-type: none"> <li>✓ Review these processes on a semiannual basis.</li> </ul> </li> <li>2. Document how Confidential (Level 1) information flows into and out of the local business unit and local applications. <ul style="list-style-type: none"> <li>✓ Review this documentation on a semiannual basis.</li> <li>✓ File a copy of the current documentation with the local IT Unit Executive/Head and the Unit Security Liaison.</li> <li>✓ The relevant IT Unit Executive/Head will be responsible for fulfilling this requirement for any campus-wide application or service that handles Confidential (Level 1) information.</li> </ul> </li> <li>3. When a unit grants any non-governmental external entity access to Confidential (Level 1) information, that entity must provide documentation of: <ol style="list-style-type: none"> <li>a. how this information will be transmitted, processed, stored and secured; and</li> <li>b. how such information is monitored and what incident response mechanisms are in place.</li> </ol> </li> <li>4. Review this documentation on an annual basis.</li> <li>5. Follow a documented process for disposal of Confidential (Level 1) information when no longer needed for legal, regulatory, or business needs. <ul style="list-style-type: none"> <li>✓ Ensure that local and HSC information retention guidelines are met.</li> <li>✓ This process needs to include an approach to information / media</li> </ul> </li> </ol>

	<p>destruction.</p> <ul style="list-style-type: none"> <li>✓ Review this documentation on an annual basis.</li> <li>✓ File a copy of the current documentation with the local IT Unit Executive/Head and the Unit Security Liaison.</li> </ul> <p>6. All users with access to Confidential (Level 1) information must execute a yearly attestation of the awareness of the relevant policies, risk, and protective measures.</p> <ul style="list-style-type: none"> <li>✓ An individual's electronic access to Confidential (Level 1) information does not convey any right to share that information with unauthorized personnel.</li> </ul> <p>7. Any systems requiring security controls beyond these baseline standards should refer to the HSC IT Security policies for ePHI. NOTE: The current (3/2010) 50 HSC IT Security policies for ePHI are being reviewed for inclusion under the new policy framework to provide elevated security requirements not included in these baseline standards.</p>
--	--

**ADDITIONAL ENCRYPTION REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION**

<p><b>Additional Encryption Requirements for Confidential (Level 1) Information</b></p>	<ol style="list-style-type: none"> <li>1. Confidential (Level 1) information must be encrypted when it is transmitted over non-HSC networks or any HSC network defined as public or untrusted. <ul style="list-style-type: none"> <li><input type="checkbox"/> Suggestion: Whenever feasible, it should also be encrypted when transmitted within HSC networks.</li> </ul> </li> <li>2. Confidential (Level 1) information must be encrypted when it is transmitted via e-mail. <ul style="list-style-type: none"> <li>✓ This applies to such information either in the body text or in an attachment.</li> <li>✓ While new versions of Microsoft Office (i.e., Office 2007 and 2010) include a facility for appropriately strong encryption of e-mail attachments, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may or may not fulfill this requirement.</li> <li>✓ Note: Other services may be developed upon request to provide a secure, Web-based vehicle for exchanging files with other individuals holding HSC NetIDs.</li> </ul> </li> <li>3. Confidential (Level 1) information may not be transmitted via instant messaging (AIM, etc.), text messaging (SMS), or other similar communication methods.</li> <li>4. Confidential (Level 1) information must be encrypted when it is accessed via the web.</li> <li>5. If passwords that grant access to Confidential (Level 1) information are stored on a networked device, they must be encrypted.</li> </ol> <p>While new versions of Microsoft Office (i.e., Office 2007 and 2010) include a facility for appropriately strong encryption, the password-</p>
---	---

	protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may or may not fulfill this requirement.
--	---

**Document Reviewed and Accepted:**

**Barney D. Metzner**

**Signed June 23, 2010**

\_\_\_\_\_  
**HSC Information Security Officer (ISO)**

\_\_\_\_\_  
**Date**

**ATTACHMENTS**

None.