

## UNM Data Encryption

**Date Issued:**

**Supersedes:** This is a new standard.

**Responsible Executive:** CIO.

**Responsible Office:** Office of the CIO.

**Contact:** For questions about this standard, please contact the Director, Information Assurance. To report violations of this standard, please call the IT Security Incident hotline, (505) 277-0930, or email the Information Assurance team at [security@unm.edu](mailto:security@unm.edu).

**Summary:** All UNM Data<sup>1</sup> must be assessed and classified according to its business or economic value to the University and its security/confidentiality requirements. The resulting classification will, in turn, facilitate applying the appropriate administrative, physical, and technical safeguards and security controls<sup>2</sup>. Any and all UNM Data that has been categorized as “E Class”<sup>3</sup> (requiring encryption) must then be encrypted when at rest as well as when in transit per this standard or via pre-approved alternative and comparable (or more stringent) encryption methods.

---

<sup>1</sup> “UNM Data” is defined as any and all data that is created in the course of UNM operations as well as data that is entrusted to UNM for business, educational or research purposes (e.g. Social Security Number, bank account number, credit card information, health, educational records, etc.)

<sup>2</sup> For example, the data may be required to be encrypted, or it may only be required to be kept confidential among UNM personnel who have a need to know.

<sup>3</sup> UNM Data Classification Standard defines 3 categories of data--each of which have their own administrative, hardware and software safeguard requirements. See <http://cio.unm.edu/standards/DataClassificationStandard041608.pdf>

**Why this standard exists:**

- a) Federal laws and regulations mandate the safeguarding of personal financial and health information<sup>4</sup> and, in some instances, require that encryption be used to render the data unreadable by unauthorized parties.
- b) The Payment Card Industry (PCI) Data Security Standard<sup>5</sup> mandates that cardholder data be encrypted whenever transmitted across an open, public network and that, at a minimum, the Primary Account Number (PAN)<sup>6</sup> be “unreadable anywhere it is stored.”
- c) External UNM audit finding 2007-06 “IT Security Recommendations”:

*“We recommend that hard drives on which sensitive data, specifically financial or student records, and employee information is held, and that are owned by the University, are encrypted to protect the sensitivity of the data. This would prevent access to the University’s data even if a computer is stolen or left unattended for a period of time. Workstations and laptops that house sensitive data, are password protected, lock out after a certain number of minutes of inactivity, and have encrypted hard drives reduce the risk of information being stolen or compromised.”*

**Audience:** All faculty, staff, student workers, contractors, and vendors working with UNM Data.

**Responsibilities:** Every University employee, faculty, student, and staff member is affected by this standard as are contactors, vendors and UNM affiliates who access “E Class” UNM Data; however, it is the responsibility of each Data Owner and Data Steward to ensure that the standard is implemented and followed.

**Website address for this standard:** <http://cio.unm.edu/standard>

---

<sup>4</sup> The Financial Services Modernization Act of 1999 (aka Gramm-Leach-Bliley Act) GLBA Safeguards Rule, 16 CFR Part 314; The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Health Insurance Reform: Security Standards, 45 CFR Parts 160, 162, and 164.

<sup>5</sup> The Payment Card Industry Data Security Standard, Version 1.1, [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

<sup>6</sup> While the UNM Lobo Card is not issued by a financial services organization such as Visa or MasterCard, one can argue that, when its LoboCa\$h function is used, the Lobo Card resembles a financial instrument and, as such, its account number should be managed with the same safeguards as a Visa or MasterCard PAN.

---

## Table of Contents

I. Standard .....	3
II. Recommended Products.....	4
III. Related Documents .....	5

---

### I. Standard

Any and all UNM Data that has been categorized as “E Class” (requiring encryption) must be encrypted when at rest as well as when in transit per this standard or via pre-approved alternative and comparable (or more stringent) encryption methods.

Any encryption product used to safeguard UNM Data must be validated by the National Institute of Standard and Technology (NIST) as complying with the Federal Information Processing Standard 140-2 (Security Requirements for Cryptographic Modules)<sup>7</sup>.

The use of an encryption algorithm that is not on the federal government list of approved methods will be considered acceptable so long as:

- a) The hardware or software safeguard (i.e. encryption product) uses an encryption algorithm that is a published, open standard which has withstood at least three years of peer review, and
- b) The product (and its algorithm) has been pre-approved by the UNM Director of Information Assurance. Requirements for pre-approval of a non-compliant encryption product should include a documented business need and context, a brief explanation as to how this non-standard product will be supported and maintained, and a statement indicating that no federally-approved encryption product or encryption product already in use across campus will meet the University’s or the particular College or Department’s requirements; *or*
- a) The product (and its algorithm) has been pre-approved by the UNMH IT Security Officer and is being used within the UNM Hospital or has been pre-approved by the HSC IT Security Officer and is being used within the UNM Health Sciences Center.

---

<sup>7</sup> Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

## II. Recommended Products<sup>8</sup>

<b>For Data-at-Rest</b>	
<b>Whole Disk Encryption</b>	
Pointsec for PC with AES Encryption	Microsoft Windows XP, 2000, & Vista
Bitlocker <sup>9</sup>	Microsoft Vista
FileVault <sup>9</sup>	Mac OS X
Pointsec for Linux	Linux
LUKS with AES	Linux
<b>File-level Encryption</b>	
PGP/GPG	Microsoft Windows, Mac OSX, Linux
TrueCrypt	Microsoft Windows, Linux
Loopback Encrypted File System w/ AES	Linux
Pointsec Media Encryption	Microsoft Windows XP, 2000
<b>For Data-in-Transit</b>	
SSH	All Operating Systems
SSL/TLS	All Operating Systems
IPSEC or SSL VPN	All Operating Systems

<sup>8</sup> As of June 2008. As the IT UNM and IT Governance units continue their evaluation and vetting of various encryption solutions, these recommendations may change.

<sup>9</sup> Cannot encrypt start-up or boot volumes; therefore, it is recommended that "E Class" data be stored on a separate volume.

### III. Related Documents

NIST Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules,  
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

Payment Card Industry (PCI) Data Security Standard, Version 1.1, September 2006,  
[https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

UNM Policy 2520 “Computer Security Controls and Guidelines”,  
<http://www.unm.edu/~ubppm/ubppmanual/2520.htm>

UNM Policy 2550 “Information Security”, <http://www.unm.edu/~ubppm/ubppmanual/2550.htm>

UNM Information Technology Standard – Data Classification,  
<http://cio.unm.edu/standards/DataClassificationStandard041608.pdf>

UNMH Administration\HSC Compliance and HIPAA Policy,  
[http://hospitals.unm.edu/policies\\_and\\_procedures/](http://hospitals.unm.edu/policies_and_procedures/)

UNM HSC 4.10 – Encryption – ePHI,  
[http://hospitals.unm.edu/policies\\_and\\_procedures/docs/Administration/HSC%20Compliance%20and%20HIPAA/4,10-Encryption-ePHI.pdf](http://hospitals.unm.edu/policies_and_procedures/docs/Administration/HSC%20Compliance%20and%20HIPAA/4,10-Encryption-ePHI.pdf)