

UNM Data Classification

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.

Summary: All UNM Data¹ 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 controls².

Why this standard exists: Without knowing the business or economic value, the security requirements, and/or the privacy requirements of UNM Data, Data Stewards may not know what levels of security should be applied. Once UNM Data are assessed, the security and privacy requirements are defined, and the data classifications are assigned, Data Stewards will have a better understanding of what administrative, physical, and technical safeguards are required to ensure the confidentiality, integrity, and availability of said data.

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

Responsibilities: Every University employee, faculty, and staff member is affected by this standard; however, it will be the responsibility of each Data Steward to ensure that the standard is implemented and followed.

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

¹ "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.)

² 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.

Table of Contents

I. Scope	3
II. Suggested Use	4
III. Data Classes.....	6
IV. Examples	9
V. Roles & Responsibilities.....	10
VI. Definitions.....	11
VII. Related Documents	12
VIII. Appendix A – Data Classification Worksheet	13
IX. Appendix B – Data Classification Flowchart	14

I. Scope

1. This standard applies to all UNM Data, independent of
 - a. The University organization, contractor, or vendor which manages it, creates it, or adds value to it (i.e. ITS, UNMH, Colleges, Departments, TouchNet, etc.),
 - b. The manner, media, or environment in which the data resides (i.e. centrally-managed, distributed data, mainframe systems, servers, personal computers, CD-ROM, DVDs, personal digital assistants, mobile storage devices, flash drives, phones, digital, paper reports, email, etc.)
 - c. The form in which the data exists (i.e. text, graphics, video, voice, paper, etc.), or
 - d. The method by which the data is stored, accessed or transmitted (i.e. data-at-rest, data-in-transit, across the wire, or via wireless transmission, etc.)
2. All UNM Data must be classified into one (1) of three (3) categories:
 - a. “**E Class**” (for data which must be **encrypted**),
 - b. “**C Class**” (for data which must be kept **confidential**), or
 - c. “**P Class**” (for data which may be released to the **public**).
3. Based on the data classification, the associated or appropriate administrative, physical and technical safeguards (i.e. security controls) must be applied.
4. All data classifications have associated safeguards.
5. Some data classifications have more stringent safeguard (i.e. security) requirements than others.
6. The safeguard (i.e. security) and privacy requirements of all UNM Data should be defined (which includes establishing the data’s value, determining all legal requirements, and determining the risk of harm from disclosure.)
7. Ultimately, it is the Data Owners’ responsibility for classifying the data for which they are responsible (and for ensuring that the appropriate safeguards are applied to the data.)
8. Data Owners are permitted to delegate the responsibility for data classification to those persons having Data Steward or Data Custodian responsibilities.
9. This standard does not address what specific technological safeguards must be applied to comply with a data classification. Such guidelines and recommendations need to be developed and kept current.
10. This standard also does not address any budgetary challenges associated with compliance.

II. Suggested Use

This standard should be used as a guide by UNM Data Owners, Data Stewards, Data Custodians, and Data Users during their efforts to discern and decide which information security safeguards are the most appropriate for the data they create, manage, use, share, and delete. It is envisioned that some form of the following steps will be taken during this data classification exercise:

1. Identify Data Owners,
2. Identify Data Stewards & Custodians,
3. Identify all of the information systems or computer applications that are within the purview of the aforementioned Data Owners, Stewards and Custodians,
4. Group or categorize as much data as possible (i.e. financial data, student records),
5. Note any specific data elements within those groupings that are already known to have particular security or privacy requirements (i.e. non-directory FERPA data, credit card numbers),
6. Develop a spreadsheet similar to **Appendix A – Data Classification Worksheet**, enter the specific data elements and grouping noted above,
7. Walk through the **Appendix B – Data Classification Flowchart** recording your decisions and rationale in the Worksheet, and
8. Once all data are classified, refer to UNM Information Security Safeguards³ for guidance on how best to manage and protect said data.

Note: While the UNM Board of Regents is ultimately responsible for the governance of the University of New Mexico, “the Board vests responsibility for the operation and management of the University in the President of the University.”⁴ The President of the University, in turn, “may redelegate authority as [s/he] deems necessary to selected administrators.”⁵

Notwithstanding any federal data ownership or federal privacy legislation, this standard assumes that either the President of the University has delegated data ownership to selected administrators or, that by the nature or scope of responsibilities of the President’s executive staff, data ownership issues can be decided.

Therefore, it is recommended that, **first and foremost** and wherever possible, consensus be developed regarding who “owns” and is administratively responsible for specific pieces of data or that, at a minimum, guiding principles be developed that will help determine when a particular piece of data is “owned” by one administrative unit and when it is “owned” by another. On the other hand, if consensus can be reached regarding the data classification of shared data, then identifying a single Data Owner may not be necessary.

³ To be developed.

⁴ N.M. Const. art. XII, § 13; NMSA 1978, §§ 21-1-1 *et seq.* and 21-7-1 *et seq.* and § 1.1 Responsibilities of the Board of Regents, UNM Board of Regents’ Policy Manual, <http://www.unm.edu/~brpm/r11.htm>

⁵ § 3.1 Responsibilities of the President, UNM Board of Regents’ Policy Manual, <http://www.unm.edu/~brpm/r31.htm>

The following is **an example** of a “SSN Ownership” guiding principle:

1. When a Social Security Number (SSN) is used for Financial Aid purposes, it is considered to be “owned” by the EVP for Academic Affairs & Provost;
2. When a SSN is used for employee tax purposes or to uniquely identify a student athlete, it is considered to be “owned” by the EVP for Administration, COO & CFO;
3. When a SSN is used for personal health information, it is considered to be “owned” by the EVP for Health Sciences;
4. When a SSN is used for donor tax purposes, it is considered to be “owned” by the VP for Advancement; and
5. When a SSN is collected and stored for multiple simultaneous purposes, it is considered to be a shared University digital asset whose data classification (and security safeguards) must be agreed to by all interested parties.

III. Data Classes

Classification	“Quick” Security Requirements	Definition & Suggested Minimum Security Requirements ⁶
E	Encrypt	<p>“E Class” data <i>must be</i> encrypted when at rest electronically (i.e. when stored in a database, in a file, or on a mobile device), or when in transit electronically (i.e. when transmitted, sent or emailed.)</p> <p>“E Class” data <i>must never be</i> emailed in cleartext⁷ and, if faxed, should only be done so in a previously-agreed upon secure manner⁸.</p> <p>Documents or mobile devices containing “E Class” data</p> <ul style="list-style-type: none"> • <i>must be</i> stored in a locked medium or facility when not in use, • <i>must never be</i> exposed to or accessible by the general public, • <i>must be</i> in a sealed⁹ container/envelope regardless if mailed or shipped externally or via inter-campus mail, and • <i>must be</i> disposed of in a manner such that they are permanently unreadable or undecipherable. <p>“E Class” is reserved for data that are either required to be encrypted per federal or state laws, per legal agreement, or per Data Steward decision.</p> <p>One example of “E Class” data is a payment card’s Primary Account Number¹⁰ or PAN (which is often referred to as the credit card number.)</p> <p>Note: Currently, there is no federal law or New Mexico state statute¹¹ requiring Social Security Numbers (or other personal information¹²) be encrypted; however, proposed federal legislation would require UNM to notify persons if “a significant risk of identity theft exists as a result of a breach of security”.¹³ Furthermore, proposed federal legislation states that “the encryption of data . . . shall establish a presumption that no reasonable risk of identity theft . . . exists following a breach of security”.¹⁴</p>

⁶ Additional security requirements may apply and UNM Information Security Safeguards need to be developed.

⁷ “In data communications, **cleartext** is the form of a message or data which is in a form that is immediately comprehensible to a human being without additional processing.” <http://en.wikipedia.org/wiki/Cleartext>. Last accessed on March 22, 2008.

⁸ Additional security requirements may apply. For example, the UNM HSC Compliance Office should be conferred insofar as ePHI and PHI security requirements.

⁹ “Sealed” includes using the envelope’s adhesive/glue or stapling – enclosing the data in such a manner that the recipient can tell if the container/envelope has been opened.

¹⁰ See Payment Card Industry (PCI) Data Security Standard, Version 1.1, September 2006, https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

¹¹ As of February 2008, 38 states have enacted some sort of breach notification law whereas New Mexico has not.

¹² See “Additional Definitions” section below for definition of “personal information.”

¹³ Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007).

¹⁴ Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007)

		<p>And California's Senate Bill 1386, upon which most states' breach notification statutes are based, modified California Civil Code requiring the disclosure of "any breach of the security of . . . data to any resident of California whose <u>unencrypted</u> personal information was, or is reasonably believed to have been, acquired by an unauthorized person."¹⁵ (emphasis added) It is for these reasons that it is <u>strongly recommended</u> that non-public "personal information" be defined, categorized as "E Class" data, and be encrypted/handled as noted above; however, it is also recommended that such decisions be left up to the Data Owners and not made lightly.</p>
Classification	"Quick" Security Requirements	Definition & Suggested Minimum Security Requirements ¹⁶
C	Keep Confidential	<p>"C Class" data <u>may be encrypted</u> when at rest electronically (i.e. when stored in a database, in a file, or on a mobile device), or when in transit electronically (i.e. when transmitted, sent or emailed.)</p> <p>A general statement of whether "C Class" data should be permitted to be faxed or emailed in cleartext or whether this data must be encrypted cannot be made without considering the context in which the data is being transmitted and the technology being used.</p> <p>It is recommended, however, that if "C Class" data is faxed or emailed <u>without</u> being encrypted,</p> <ul style="list-style-type: none"> • the receiving facsimile machine <u>should not be</u> accessible to the general public, • the recipient email addresses <u>should only be</u> official UNM email addresses (i.e. @unm.edu), official contractor or vendor email addresses, • The recipient email addresses <u>should not be</u> "publically-available" email addresses such as those managed by gmail, hotmail, AOL, Yahoo!, Quest, Comcast, etc., and • The email <u>should not be</u> accessed via an unsecure wireless network without the use of appropriate security controls that ensure the email's contents stay confidential and are not accessible by unauthorized persons. <p>Documents and mobile devices containing "C Class" data</p> <ul style="list-style-type: none"> • <u>should be</u> stored in a locked medium or facility when not in use, • <u>must never be</u> exposed to or accessible by the general public, • <u>should be</u> in a sealed container/envelope regardless if mailed or shipped externally or via inter-campus mail, and • <u>must be</u> disposed of in a manner such that they are permanently unreadable or undecipherable. <p>"C Class" is reserved for data whose unauthorized disclosure would</p>

¹⁵ California Civil Code § 1789.29

¹⁶ Additional security requirements may apply and UNM Information Security Safeguards need to be developed.

		<p>be a violation of federal or state laws, University legal agreements, or University policy; <u>whose disclosure may cause irreparable harm to the University</u>, a faculty member, a student, a staff member, alum, or business associate; and whose confidentiality is deemed warranted by its Data Owner.</p> <p>One example of “C Class” data is the non-directory portion of a student’s education record¹⁷. Such data may be amended to include some or all of a student’s public directory information if so requested by a student.</p> <p>“C Class” data may also include documents which, at first glance, may be considered to be Public Records in accordance with New Mexico “Inspection of Public Records Act”, NMSA 1978, Chapter 14, Article 2, but, upon further consideration by either the Data Owner or UNM’s Public Records Custodian, are deemed confidential since their disclosure may cause irreparable harm to the University (e.g. UNMH security diagrams, the location of research compounds that may be hazardous.)</p>
Classification	“Quick” Security Requirements	Definition & Suggested Minimum Security Requirements ¹⁸
P	Public Access <u>May</u> Be Granted	<p>Data to which the general public <u>may</u> be granted access in accordance with the New Mexico “Inspection of Public Records Act”, NMSA 1978, Chapter 14, Article 2, UNM Board of Regents' Policy 2.17, Public Access to University Records, and UNM Policy 2300, Inspection of Public Records.</p> <p>Data whose unauthorized disclosure would not be a violation of federal or state laws, University legal agreements, or University policy; whose disclosure would not cause irreparable harm to the University, a faculty member, a student, a staff member, alum, or business associate; and whose confidentiality cannot be justified by its Data Owner.</p> <p>One example of “P Class” data is an UNM employee’s office location and phone number¹⁹.</p> <p>Note: UNM employees have a fiduciary responsibility to maintain the integrity and availability of all UNM Data including “P Class”.</p>

¹⁷ Family Educational Rights and Privacy Act Regulations (FERPA), 34 CFR Part 99.

¹⁸ Additional security requirements may apply and UNM Information Security Safeguards need to be developed.

¹⁹ There may be occasions in which UNM Administration, University Counsel, the UNM Police Department, or an appropriate University office determines that an employee’s office location or phone number should not be released to the general public (such as stalking, when restraining orders exist, when an employee has a reasonable fear or concern of being harmed if such data is readily available to the public, etc.)

IV. Examples

Classification	Example	Business Driver or Justification
E	Social Security Number, when "transmitted electronically"	Per § 5 "Use of SSNs" in the draft of UNM Policy 2030, dated 02/11/2008 ²⁰
E	A payment card's Primary Account Number or PAN (which is often referred to as the credit card number)	Per Payment Card Industry (PCI) Data Security Standard, Version 1.1, September 2006. ²¹
C ²²	Drivers license information, Financial aid information, Bank account numbers, Credit and payment history, Income records, Date and location of birth, Account balances, and Automated clearing house (ACH) numbers	Per § 1 "General" in the draft of UNM Policy 2550 "Information Security Program", dated 02/20/2008.
C ²³	Electronic Personal Health Information (aka ePHI)	Per UNM Hospitals Policies and Procedures, <i>Administration\HSC Compliance and HIPAA</i> .
C	"Education records", and "Student records" ²⁴	Per UNM Student Records Policy (which was developed to comply with The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99.)
C	Candidate-for-employment information	See UNM Board of Regents' Policy 6.7 Confidentiality of Employment Applications concerning what and when particular candidate information is permitted and not permitted to be made public.
C	University Presidential candidate or nominee information	See UNM Board of Regents' Policy 1.4 Appointment of the President of the University concerning what and when particular candidate/nominee information is permitted and not permitted to be made public.
P	Employee office location, Employee phone number,	Data to which the general public may be granted access in accordance with the New Mexico "Inspection of Public Records Act", NMSA 1978, Chapter 14, Article 2 , UNM Board of Regents' Policy 2.17, Public Access to University Records , and UNM Policy 2300, Inspection of Public Records .

²⁰ As of 3/24/08, in draft form only.

²¹ See Payment Card Industry (PCI) Data Security Standard, Version 1.1, September 2006, https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

²² It is recommended that these data be considered for encrypted especially if used in conjunction with the owner's name. See "Additional Definitions" section below for definition of "personal information."

²³ Per UNMH Administration\HSC Compliance and HIPAA Policy §§ 4.10 Encryption-ePHI, 4.11 Encryption and Decryption-ePHI, and 4.12 Transmission Security-ePHI, some ePHI may be required to be encrypted and may warrant an "E Class" classification

²⁴ Except those UNM Data elements listed in § 10.0 Directory or Public Information Categories of the UNM Student Records Policy (unless a student has asked for some or all of the § 10.0 data elements to be kept private).

V. Roles & Responsibilities

Role	Description
Data Owner	<p>Senior UNM official (or designee) having</p> <ul style="list-style-type: none"> (a) Policy-level and data-management planning responsibility for data within their functional areas, (b) Management responsibilities for defined classes of UNM Data, or (c) Overall or final responsibility for a particular information system. <p>Example(s):</p> <ul style="list-style-type: none"> • EVP for Academic Affairs & Provost: Data Owner of all student educational data. • EVP for Administration, COO and CFO: Data Owner of all Human Resource data, financial data, physical plant data, and Auxiliary Enterprises data.
Data Steward	<p>UNM officials (or designees) having direct operational-level responsibility for information management – usually department directors. Data Stewards are responsible for data access and policy implementation issues and, because of separation of duty issues, are not considered to be the owners of the data/system.</p> <p>Workforce constraints may require a system's Data Steward to also be the system's Data Custodian (i.e. the person responsible for establishing data access policies and procedures may be the same person tasked with following the policies and procedures and implementing the appropriate access controls.)</p>
Data Custodian	<p>The information agent having responsibility for any of the following: maintaining the data, managing the means by which the data is collected or stored, granting access privileges to Data Users as authorized by Data Owners or their designees (usually the Data Stewards), backup and recovery processes, providing physical security for said UNM Data.</p> <p>Workforce constraints may require a system's Data Custodian to also be the system's Data Steward (i.e. the person responsible for following policies and procedures and implementing the appropriate access controls may be the same person tasked with establishing the data access policies and procedures.)</p>
Data User	<p>Individuals who need and use UNM Data as part of their assigned duties or in fulfillment of assigned roles or functions within the UNM community. Data users may also be primary data entry personnel who are, by the nature of the task, responsible for the data's initial integrity.</p>

VI. Definitions

Administrative Safeguards	Administrative policies and procedures designed to manage the selection, development, implementation, and maintenance of security measures and to manage the conduct of UNM's workforce, contractors, vendors and business associates.
Availability	<p>Availability means that the data, information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed.</p> <p>Even "P Class" data that may be released to the public can have availability requirements. For example, as faculty, students and staff become more reliant on the online directory for contact information, the more important the availability of that computer application becomes.</p>
Confidentiality	Data that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to do so, and only when there is a genuine need to do so. A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.
ePHI	Any Protected Health Information (PHI) which is created, stored, or transmitted <i>electronically</i> .
Goals of Information Security	To appropriately address the confidentiality, integrity and availability (CIA) requirements of information and data.
Integrity	<p>Data that is considered to have integrity must never be created, changed, or deleted without authorization and intent.</p> <p>Even "P Class" data that may be released to the public can have integrity requirements. For example, as faculty, students and staff become more reliant on the online directory for contact information, the more important the quality and correctness of that data becomes.</p>
Personal Information	<p>Most states mirror California's Security Breach Information Act, SB 1386, and define "personal information" as individual's first name (or first initial) and last name in combination with any one or more of the following data elements:</p> <ol style="list-style-type: none"> (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Physical Safeguards	Physical measures, computer hardware, software, technologies, policies and procedures designed to protect UNM's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
Technical Safeguards	Any technology, computer hardware, software, network, security mechanisms, or security services that protect and control access to data.

VII. Related Documents

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, 34 CFR Part 99,
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

New Mexico "Inspection of Public Records Act", NMSA 1978, Chapter 14, Article 2,
<http://www.nmcpr.state.nm.us/info/14-2NMSA.pdf>

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

State of California Security Breach Notification Act (SB 1386),
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

UNM Board of Regents Policy 1.4 "Appointment of the President of the University",
<http://www.unm.edu/~brpm/r14.htm>

UNM Board of Regents Policy 2.17 "Public Access to University Records",
<http://www.unm.edu/~brpm/r217.htm>

UNM Board of Regents Policy 6.7 "Confidentiality of Employment Applications",
<http://www.unm.edu/~brpm/r67.htm>

UNM Policy 2300 "Inspection of Public Records",
<http://www.unm.edu/~ubppm/ubppmanual/2300.htm>

UNM Policy 2510 "Computer Use Guidelines",
<http://www.unm.edu/~ubppm/ubppmanual/2510.htm>

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

UNMH Administration\HSC Compliance and HIPAA Policy,
http://hospitals.unm.edu/policies_and_procedures/

UNM HSC Clinical Operations - Right to Access of Protected Health Information by the Patient
[http://hospitals.unm.edu/policies_and_procedures/docs/Administration/General/Right to Access of Protected Health Information by the Patient.doc](http://hospitals.unm.edu/policies_and_procedures/docs/Administration/General/Right%20to%20Access%20of%20Protected%20Health%20Information%20by%20the%20Patient.doc)

UNM HSC Clinical Operations - Use and Disclosure of Protected Health Information Policy
[http://hospitals.unm.edu/policies_and_procedures/docs/Administration/Security-Safety/Use and Disclosure of Protected Health Information \(PHI\).doc](http://hospitals.unm.edu/policies_and_procedures/docs/Administration/Security-Safety/Use%20and%20Disclosure%20of%20Protected%20Health%20Information%20(PHI).doc)

IX. Appendix B – Data Classification Flowchart

