UNM | Office of the CIO

UNM Data Center and Server Room Standard

IT Standard Issued: Draft of February 8, 2016
Effective Date:
Responsible Executive: UNM Chief Information Officer (CIO)
Responsible Office: UNM CIO
Contact: Director of IT Platforms, Information Technologies Department

Purpose of the Standard

This standard is intended to describe minimum requirements based on uptime, availability and security that UNM Data Center and Server Room facilities need to meet in order to guide managers of these facilities in appropriate safeguards for University and individual data and information. This standard applies whether the facility is externally facing to the Internet, or internally-facing to an intranet. The types of data stored or processed in the facility also drive facility management decisions. Guidelines for various data in relation to computing facilities are also included in the standard.

The standard defines tiers that articulate the minimum physical infrastructure requirements, based on uptime and potential impact that UNM facilities must meet. The standard also describes minimum physical security requirements for computer infrastructure and resources that host protected data.

Departments and/or units may choose to implement more restrictive, but not less-restrictive measures in facility management. The Office of the CIO requests that management principles that vary from the standard be filed with the CIO.

Definition of Data Center / Server Room

For the purposes of this standard, "Data Center" or "Server Room" refers to any physical space, room or building, where computers and related equipment (such as servers, racks, electronic storage, or communications networking) and any associated physical or technology-based infrastructure (conditioned power, cooling or humidity control, or fire suppression) owned or managed on behalf of UNM are operated to serve the mission of the University of New Mexico.

Who Is Affected by the Standard?

The standard applies to entities that design, install, monitor, maintain, and/or decommission UNM computing equipment and associated infrastructure that stores, processes, provides, or transmits information or data that is served up via this IT infrastructure for:

- UNM departments, business units or affiliates.
- UNM faculty, staff, students, and/or vendors.
- UNM researchers

Scope of the Standard

The standard addresses the following areas:

- Physical space or facility housing technology assets, such as servers, which are used to process, store, transmit or backup University or personal information.
- Protection and security of these technology assets
- Protection and security of information assets
- Power capacity, quality and availability of power
- Physical security such as access, surveillance, monitoring
- Environmental controls such as cooling
- Availability or Up-time for mission critical resources
- Access to the facility by people and the network
- Network cabling within the facility

Excluded from the standard are the following:

- Individual workstations, desktops or mobile devices
- Network Security (Firewalls, Intrusion Detection or Prevention systems, Monitoring or non-repudiable system logging)
- Network closets or wiring centers
- Data governance and/or classification of data
- Administrative and technical safeguards of protected data classes
- Approval of facilities assignment to tiers

Roles & Responsibilities Regarding the Standard

- **Office of CIO**: Ensure currency, correctness and appropriate periodic review of the Standard by chartering Technical Review Committee as needed and specifying desired outcomes.
- **Technical Review Committee Chair**: Convene and manage the committee to deliver work chartered by the CIO.
- **Department Heads of UNM Departments Managing a Data Center or Server Room**: Confirm in writing to be filed in the Office of the CIO the appropriateness of the Tier and physical security required for the information processed, transmitted and stored by that Department's facility.
- **Administrators, Staff, Faculty & Principal Investigators**: are responsible for the data being processed, transmitted and stored, and for selecting the appropriate physical security environments.
- **Internal Audit**: Determine compliance with this standard during the audit of departments with data centers/server rooms.

Process for Review or Update of the Standard

- **Compensating Controls** – The acceptability of compensating controls to these standards in Departments will be determined by Internal Audit.
- **Review or Update** - Request for review or update of the standard can be requested by contacting the Office of the CIO or the Contact identified above. They will then convene appropriate parties to develop an updated version of the standard for approval.
- **Process documentation** development
    - Each site will have policies defining roles, responsibilities, and performance standards

- Each site change will require a review and update of all documentation
- Site Books will be developed for each site covering all tasks and responsibilities required to support that site. This will include all policies, site standards, and procedures

- **Review, update, and replacement of existing documentation**
  - Policies and procedures are reviewed and updated yearly as needed
  - Each standard has a Contact Person who is responsible to the Accountable Office for maintaining the Standard and related documents.
  - The Contact Person or Accountable Office for the standard can communicate all changes to the policy or appendices to the IT Agent and managers community. It will then be the responsibility of IT agent and managers groups to notify and inform all other IT organizations under their units.
  - Changes to the standard are required to have a period of campus input.

Compliance

- Entities to which the standard applies will develop their own approach, plan and funding strategy to achieve compliance.
- Entities to which the Standard applies are subject to audit against this standard.
- This standard has been developed under and is subject to the UNM policies referenced at the end of this standard.

Standard Specifications

There are two areas of specification addressed by the Data Center Standard: 1) Facility Tiers and 2) Physical Data Security. It is the responsibility of the Department Head of the UNM departments that manage a data center or server room manager to identify and self-select which of the four facility tiers they will adhere and be audited against. The liability of maintaining and correctly classifying a data center or server room environment is not negated by a misclassification. Failure to maintain the physical server facility or datacenter to the chosen tier or failure to properly categorize the server room or data center to the correct tier level may have repercussions based on audit findings and are the responsibility of the agency (Unit, Department, and College) that oversees the IT resource. Physical Data Security add-ons are based on requirements dictated by the various data types (such as PCI standards). Regardless of the facility tier selected by the organization all Physical Data Security add-ons must be met.

1. Data Center & Server Room Facility Tiers (Appendix A)

Physical facilities of data centers and server rooms are grouped into Facility Tiers. Facility Tiers are recommended based on the requirements for up time and impact when the system is unavailable. The following describe the spirit of the specifications.

- **Physical Security** requirements of data stored in those facilities may drive higher levels of physical security than are specified by the facility tier levels alone.
- **Monetary values** indicate the level of responsibility in the management and protection of UNM assets. Compensating controls can be allowed to meet the intention of these requirements.
- **Availability** specifications guide managers in determining the levels of physical security for the environment.

Facility Tiers are recommended as follows:

- **Tier 1 Facility** is defined by the lowest demand for up-time and least potential impact.
    - **Recommendation:**
        - **90% availability excluding planned downtimes**
        - **Less than 25 people**
        - **Under an asset value $50,000**
        - **Should not contain data critical to departmental operation**
    - The Facility meets minimum requirement for the safe operation and maintenance of computing equipment and protection of assets. Door lock, power tap, UPS recommended.
    - An example is an individual or small group within a single unit sharing a server. The server is behind a locked door.
- **Tier 2 Facility** is defined by a need for medium up time and impact.
    - **Recommendation:**
        - **99.9% availability**
        - **Less than 10% of active UNM population**
        - **Combined asset value under $200,000**
    - This facility meets Tier 1 security plus UPS, basic environmentally-controls for temperature and humidity.
    - An example would be a single departmental server, shared drive, shared application, web site hosting.
- **Tier 3 Facility** is defined by a need for high up time and impact.
    - **Recommendation:**
        - **99.99% availability**
        - **Less than 30% of active UNM population**
        - **Combined asset value under $500,000**
    - Power & air redundancy, environmental controls and backups for cooling & humidity.
    - Examples could include larger college-level operations affecting multiple departments, faculty, students, or researchers.
- **Tier 4 Facility** is defined by a need for the highest levels of up-time and impact.
    - **Recommendation:**
        - **99.999% availability**
        - **Greater than 30% of active UNM population**
        - **Combined asset value over $500,000**
    - Highest levels of power and environmental redundancy, access controls, physical security and monitoring.
    - Example would include enterprise data centers serving whole population segments of faculty, researchers, students and/or staff.

Facility Tier standards for physical facilities and support services are defined in the following areas for each tier above in Appendix A.

- **Physical Facilities** address structures that need to be in place by tier for Safety, Physical Access Controls, Electrical Feeds, Temperature & Humidity Controls, Networking Feeds, Raised Floor, Server Cabinet Systems, Cable Plant, and Cable Management.
- **Support Services** allow for the efficient and effective deployment of services to meet UNM community administrative, academic and research needs reliably and securely.

These services include Server Installation, Network Layout, Server Removal, and Administrative services.

2. Physical Data Security (Appendix B)

Physical Data Security addresses information governed by law and/or University Policy, as well as references the Data Classification Standard (found http://cio.unm.edu/standards/docs/DataClassificationStandard041608r.pdf). Each facility collecting, transmitting or storing data in these classification, must meet the physical security requirements for that data as specified in Appendix B. Data Types are defined in the Glossary. Physical security requirements for data types are found in Appendix B and address physical safeguards.

2.1 Special Considerations for Researchers and Research Data

Researchers are responsible for identifying and utilizing appropriate facilities and protections in order to secure their research data. Toward this end, it is recommended that researchers perform an annual ***value assessment*** of their research data with respect to monetary, IP, or other suitable criteria. This will aid in performing the subsequent risk and impact analysis for determining the appropriate data center Tier, as described above, for storing their data.

- Research data can change from needing very little or no security, to some security, to the highest levels of security (e.g., patentable data/results).
- The research data lifecycle can operate in reverse, and go from high-security needs to no security (e.g., data embargo status may change).
- Legal guidelines (e.g. HIPAA, FERPA) supersede or prevail over any research guidelines.

As part of this data assessment, researchers should consider the impact that their self-classification might have on other researchers, projects, and facilities. For example, an inappropriate designation (too low or too high) could put another researcher at risk; lead to unnecessary delays and costs; and could ultimately erode research participation and collaboration.

Annual re-assessments will be designed to address the changing nature of a researcher's data, and impacts on shared or collaborative research and facilities.

Definitions & Glossary

See Appendix C:

References

University Administrative Policies related to data security:

- Policy 2030 SSN Policy - http://policy.unm.edu/university-policies/2000/2030.html
- Policy 2040 Identity Theft Protection Program – http://policy.unm.edu/university-policies/2000/2040.html
- Policy 2500 Acceptable Use Policy – http://policy.unm.edu/university-policies/2000/2500.html
- Policy 2550 Information Security Program – http://policy.unm.edu/university-policies/2000/2550.html
- Policy 2520 Computer Security Controls and Access to Sensitive and Protected Information - http://policy.unm.edu/university-policies/2000/2520.html

- Policy 3710 Personnel Information Disclosure Policy – http://policy.unm.edu/university-policies/3000/3710.html
- Policy 4610: Acquisition and Disposition of UNM Surplus equipment https://policy.unm.edu/university-policies/4000/4610.html
- Policy 7215 Credit Card Policy - http://policy.unm.edu/university-policies/7000/7215.html
- Policy 7710 Property Management and Control https://policy.unm.edu/university-policies/7000/7710.html
- UNM Faculty Handbook, E70: Intellectual Property Policy, http://handbook.unm.edu/section-e/e70.html
- Regents Policy Section 7.2 Internal Auditing and Compliance http://policy.unm.edu/regents-policies/section-7/7-2.html

Appendix A
Data Center & Server Room Facility Tiers
IT Data Center Standard

As of October 21, 2015

Notes on the Chart:
The Data Center & Server Room Facility Tiers below are defined in the Standard document.
Colors in the cells indicate that the safeguard is required for that tier, sometimes with annotation.
Gray cells indicate that the engagement of PPD is required or recommended.
The chart assumes that all building codes where the data center or server room is located are met.

Is data center compliant to the Standard?	Tier 4	Tier 3	Tier 2	Tier 1
I. Physical Facilities				
Safeguards and controls help assure human safety, as well as the continuity of operations of IT services. Best practice based standards for data center and server rooms help assure that IT services can be supported efficiently and effectively, so as to maximize the value and security of the services provided.				
A. Safety Controls				
1. Fire alarm and suppression system				
a. Must be designed and approved for use in data centers				
b. Must comply with all national, state, and local building codes				
c. Suppression systems must use chemicals that do not damage sensitive equipment		Recommended		
d. Suppression systems must not pose harm to building occupants	Require training	Recommended		
e. Must be maintained by qualified technicians				
f. Separate detection/suppression (chemical or gas) zone under and above raised floors and above ceiling	Require training			
2. Electrical emergency cut-off system				
a. Must be designed and approved for use in data centers				
b. Must comply with all national, state, and local building codes				
c. Must be maintained by qualified technicians				
d. Must be inspected annually by Fire Marshall				
3. Building and door security system				
a. Must be designed and approved by UNM Physical Plant and UNM Police (Policy 5010)				
b. Must comply with all national, state, and local building codes				
c. Must be maintained by qualified technicians				
d. Must be inspected annually by Fire Marshall				
e. Must have logs and reporting to separate system				
B. Physical Access Controls				
1. Door security				
a. All door access controls must be installed and maintained by UNM PPD				
b. Door access control must be maintained 24/7 and should conform to audit standards (ISO-27001)		Recommended		
c. An electronic access control system should be in place and log all access to secure data areas		Recommended		
d. Access logs should be maintained for one year and recoverable (indefinitely?)		Recommended		
e. Enforcement of strict polices and sign in/out logs is mandatory (could be via electronic controls)		Recommended		
f. Review of procedures and sign in/out logs must be performed regularly		Recommended		
g. Per National Fire Protection Life Safety Code 101, secured (egress-impeded) doors must fail open/safe in a fire emergency and have an exit mechanism installed.		Recommended		
2. Video security				
a. Allows for local and remote surveillance of secured and public areas				
b. All entrances and exits to all data center spaces and server room spaces must be covered by the video security system				
c. Recording must be accessible outside the datacenter				
d. Recording system must be self-checking or maintained and checked on a regular basis				
e. All security recordings must be saved for 30 days and archived for 365 days retrievable within 7 business days (cut via analytic tools?) (seems longer than needed - 90 days?)				
3. Granting security access (covered much by UNMBP 5010 - can't get keys without approval)				
a. Data center locations must have a visitor/non-essential staff access policy				
b. Access must only be granted to essential personnel (UNMBP 5010 & management)				
c. Visitors must be signed in and out and be supervised at all times				
d. Visitor logs should be maintained for 30 days and archives kept for 365 days retrievable within 7 days				
e. Visitors must be able to be monitored at all times		Recommended	Recommended	Recommended
f. Orientation provided to PPD/vendors/non-IT necessary access				
4. Emergency procedures				
a. All sites must maintain posted emergency procedures				
b. Emergency contact information posted and readily visible				
c. Planned and documented IT physical facilities continuity plan in place				
d. Regularly review and test emergency procedures and equipment with staff				
e. Uninterruptable emergency assistance and communication channels available (e.g. Call button in an elevator)				
5. Monitored Alarms -Needs to be discussed w/alarms & UNMPD				
a. Intrusion detection (forced entry - UNMPD - what response times can be guaranteed?)				
b. Perimeter detection (held door)				
C. Electrical Feeds - Must go through PPD project planning / Approved vendor SLA				
1. Main and step down transformers				
a. Must be located in a secure environment				
b. Must have HVAC systems to support heat load and correct humidity levels for each unit				
c. Must be maintained by a qualified technician to factory standards and be supportable by extended factory warranty				
2. Main power control panel				
a. Must be maintained by a qualified technician to factory standards				
b. Must be located in a secure mechanical room				
c. Must have HVAC systems to support heat load and correct humidity levels for each unit				
d. Must have surge suppression sufficient to prevent large surges from damaging panels and equipment supported by panel				
e. PLC must have password security				
f. PLC must have UPS support for power failure				
3. Motor control panels				
a. All controls must have automatic restart after power failure				
b. Must be maintained by a qualified technician to factory standards				
c. Must be located in a secure environment				
d. Must have HVAC systems to support heat load and correct humidity levels for each unit				
4. UPS systems				
a. UPS systems in the data center must be scalable to meet current and future needs				
b. UPS systems in the data center must have sufficient battery backup to allow for a controlled shutdown of primary systems				
c. UPS systems must be designed, installed and maintained by authorized electricians and technicians and housed in a secure location.				
d. UPS systems follow manufacturer's recommended maintenance schedule for life of device				
e. UPS systems must have bypass/redundant capability to allow for periodic maintenance				
f. UPS systems should be monitored from local and alternate sites			Recommended	

Is data center compliant to the Standard?	Tier 4	Tier 3	Tier 2	Tier 1
g. UPS systems should power down systems in the event of an outage	Recommended	Recommended	Recommended	Recommended
5. Backup batteries (battery storage)				
a. Must follow manufacture's recommendations for system to be of sufficient quality and capacity to ensure a long life thus limiting breaks in the battery strings				
b. Must be located in secure area with proper ventilation as required				
c. Must be installed and maintained by authorized technicians				
d. Must be approved for use in computer equipment UPS systems				
6. Sub-panels Must go through PPD project planning / Approved vendor SLA				
a. Must be sized to meet current and future needs				
b. Must be located in the data center to minimize power runs to desired equipment				
c. Panel maps must be maintained to reflect their most current usage				
d. Sub-panels must never be opened at the face plate by anyone other than qualified electricians				
e. All materials must be at least three feet away from sub-panels				
7. RPP (Remote Power Panel) units				
a. Must be located to maximize ease of distribution to equipment				
b. Must comply with BS/IEC/EN 60439-1				
8. Underwriter's Lab (UL) -Rated Power Taps (Note: no surege suppressors should be used)				
a. Must be sized to meet the power requirements of the device for which they are installed				
9. Power cable layout in racks/cabinet				
a. The power pathways must maintain a minimum separation from data cable pathway in accordance with ANSI/TIA-469-B Standards				
b. Equipment power cables should be the minimum required length and slack/strain management must be employed				
c. Cables must be arranged to minimize air flow disruptions				
10. Grounding systems Must go through PPD project planning / Approved vendor SLA				
a. All data center equipment must be grounded in compliance with state and local codes				
b. Data center equipment grounds must be independent of all other building grounds (such as lightning protection systems) - ??				
c. All metal objects must be bonded to ground including cabinets, racks, PDUs, CRACs, cable pathway, and any raised floor systems				
d. Ground resistance should be < 1 Ohm				
11. Monitoring system				
a. All electrical infrastructure must be monitored				
b. Monitoring systems must be configurable for structured, automated notification				
c. Central system must be located external to monitored environment and be remotely accessible				
d. Monitoring system must have analysis and reporting function				
e. System must be able to retain log files of equipment performance and incident history				
f. Monitoring systems should have edit & configuration protection capabilities				
12. Generator management - Must go through PPD project planning / Approved vendor SLA				
a. Generator must be start tested and run for at least one hour once a month				
b. A full load test and switching test must be conducted at least yearly				
c. Maintenance logs must be kept on all tests and reflect all maintenance performed				
d. All maintenance must be performed by a qualified technician to factory specifications				
e. Management must include remote alarm panel (enunciator panel)				
13. Maintenance and testing				
a. All electrical system components should be regularly inspected				
b. Main power switches, transformers, automatic transfer switches, and other major electrical system equipment must be maintained by qualified technicians per factory specifications and recommendations for service cycles.				
14. Redundancy and Maintenance				
a. Redundant power must be available if primary source fails		Recommended		
b. Bypass must be available for all electrical systems				
D. Temperature and Humidity Controls				
1. CRAC (Computer Room Air Conditioner) Units				
a. Cooling and related equipment must be sized to account for				
i. The size of the cooling load of all equipment				
ii. Sized to account for humidification effects		Recommended	Recommended	
iii. Sizing to account for appropriate future growth projections (consideration)				
iv. Adequate multi-layer air conditioning, including a backup N+1 (or N+N) system for the multi-layer DX, in case one or the other is unavailable air conditioning providing further back up by splitting cooling between chilled water and refrigerated cooling		Recommended		
b. All cooling equipment must be designed, installed, and maintained by qualified technicians that meet local and state codes. All cooling equipment must follow the vendor's recommended maintenance schedule				
c. Air filtration media should be installed at air intake points. Media should be replaced on a regular schedule based on the manufacturer recommended filter lifespan				
d. Humidity/temperature control		Recommended	Recommended	
i. Humidity and temperature must be maintained at a level that is compliant with the equipment installed on the data center floor.		Recommended	Recommended	
ii. Humidity injection units must have separate drains and be fed by conditioned water		Recommended	Recommended	
e. Cooling towers - If applicable Must go through PPD project planning / Approved vendor SLA				
i. Units must be maintained by qualified maintenance technicians following factory guidelines				
ii. Units must be in a secure mechanical yard				
iii. Units should be designed and installed to eliminate single point of failure				
iv. Tower restart after power failure must be automatic				
v. Towers must have a redundant power source to allow time for a controlled shutdown of supported areas				
f. Pump systems				
i. Units must be located in a secure mechanical room				
ii. Units should be designed and installed to eliminate single point of failure				
iii. Pumps must restart automatically after a power failure				
iv. Pumps must have an emergency power source to allow time for a controlled shutdown of supported areas				
g. Pipe system				
i. Pipe must be constructed of high quality rust- and coolant-resistant material				
ii. Pipe loops must have valves in several locations that allow sections of the loop to be isolated without interruption to the rest of the loop				
iii. Pipe loops must have isolation valves for each CRAC unit				
h. Air delivery and return management				
i. Cold air delivery must be managed such that the required amount of air can be delivered to any necessary equipment location				
ii. Hot air return must be managed to extract air directly to CRAC units without mixing with cold air delivery				
i. System monitoring				
i. All infrastructure systems supporting machine space services must be monitored 24/7			Recommended	
ii. Monitoring must be at a central location with remote monitoring capability				
iii. Monitoring system logs must be maintained				
iv. Monitoring must include humidity				
E. Raised Floor Systems - if applicable				
a. Under floor space management				

Is data center compliant to the Standard?	Tier 4	Tier 3	Tier 2	Tier 1
i. Must remain clean and corrosion free				
ii. Constant air pressure must be maintained at all times				
iii. Must remain obstruction free for proper air-flow				
iv. Flood sensors and monitoring under raised floors and in all critical areas				
b. Cleaning				
i. Must be done with vacuum cleaners equipped with HEPA/S-class filters				
ii. Must be done on a continual basis				
c. Floor structure maintenance				
i. Must be corrosion and rust free				
ii. Damaged pedestals, cross members, tiles, or missing fasteners must be replaced immediately to maintain floor integrity				
d. Floor grounding				
i. Must be separate from building ground				
ii. Must comply with all state and local codes				
F. Server Cabinet Systems - See UNM IT policy - want to narrow scope				
a. The data center site must have a standardized set of cabinets tailored to the site's specific needs				
b. Blanking panels will be installed in any unused rack space to minimize cold/hot air mixing				
c. Large servers and equipment must be installed at the bottom of the rack				
G. Cable Plant -				
1. Overhead delivery system cable layout				
a. The data room must have a system to support overhead delivery of data connections to the equipment cabinets				
b. The data pathways must maintain a minimum separation from high voltage power and lighting in Association) and in compliance with PPD Standards accordance with ANSI/TIA-469-B Standards				
2. Fiber standards:				
a. Fiber installation must use 50 Micron OM3 Laser optimized fiber				
b. All fiber installations must be labeled				
3. Copper standards				
a. Copper jumpers must be CAT6 with Booted RJ45 connectors				
b. All copper data cables must be labeled				
4. Grounding				
a. All cabinets and cable delivery pathways must be grounded in compliance with PPD Standards				
H. Cable Management				
1. Full accessibility to cables must be maintained				Recommended
2. Data pathways must maintain a minimum separation from high voltage power				Recommended
3. New cables must conform to newest standard (e.g. CAT6 in 2015)				Recommended
4. Cables should employ labeling				Recommended
5. Cables should have adequate spacing/pathway capacity				Recommended
6. Cabling must conform to UNM IT Cabling Standards or equivalent				Recommended
II. Support Services				
Standards--based support services allow for efficient and effective deployment of services to meet the academic, business, and research needs of the UNM community in an effective, secure, and reliable manner.				
A. Server Installation				
1. Power				
a. Systems with redundant power supplies must have their power cords plugged into separate power taps			Recommended	Recommended
b. Power must be isolated from data cables			Recommended	Recommended
c. Power cords must be factory certified			Recommended	Recommended
d. Power cords must be clearly labeled			Recommended	Recommended
2. Rack space				
a. Rack equipment should be loaded from the bottom up based on weight and size				
b. Equipment must be clearly labeled				
c. Data connections				
i) Cable length should be appropriate to minimize excess slack				
ii) Must be isolated from the system and rack power delivery system				
iii) Must be clearly labeled				
3. Fiber connections				
a. Fiber should be of an appropriate length to minimize excess slack				
b. Must be clearly labeled				
c. Must not exceed minimum bend radius as specified by the manufacturer				
B. Network Layout - Possibly TBD by Phase II/Other Standard				
1. Standard switch layout				
a. All networking equipment will be installed in coordination with UNM IT Networking				
b. Switches must be installed in a fashion to minimize the length of data cables required to provision a data connection				
2. Highly critical system switch layout and redundancy				
a. In the case of highly critical systems where network path redundancy is required, the systems must have redundant data circuits that connect to separate switches		Recommended		
b. Redundant switches must be plugged into separate power strips		Recommended		
C. Server Removal - Refer to UNMBP Policy 4610 on Surplusing UNM Assets				
https://policy.unm.edu/university-policies/4000/4610.html				
D. Site Procedure and Site Policy Development				
1. Process documentation development				
a. Each site will have policies defining roles, responsibilities, and performance standards				
b. Each site change will require a review and update of all documentation				
c. Site Books will be developed for each site covering all tasks and responsibilities required to support that site. This will include all policies, site standards, and procedures		Recommended		
2. Review, update, and replacement of existing documentation				
a. Policies and procedures will be reviewed and updated yearly				
b. Each policy and procedure will have an subject matter expert(s) responsible for maintaining the documents				
E. Management of Site Support Tools and Equipment				
1. Definition of equipment required				
a. Each site will create an inventory of support equipment required for that site.				
b. Each site's needs must be evaluated to determine if support equipment can be shared between sites	Recommended			
2. Storage, maintenance, and update of equipment				
a. Procedures will be developed for maintenance of site equipment				
b. Site support equipment needs will be reviewed yearly			Recommended	
c. Each site will have a defined area for storage of site equipment		Recommended		
d. A list of all sites and their equipment will be kept at each site to allow quick location of equipment that can be shifted in case of need	Recommended	Recommended		

Appendix B
Physical Security Requirement of Data Centers & Server Rooms

October 21, 2015

Please see Appendix C, Glossary, for the definitions of these terms.
If the data center or server room stores or processes the data named in the columns below, the data center needs to have the security indicated in each column, regardless of tier. This means that the legal requirements govern how data is protected physically.

Please read with the spirit of the control in mind, rather than specific technologies.

Key:
A = Must be addressed in the spirit of the requirement category.
S = Suggested or Recommended.
N/A = no recommendation or requirement

	GLBA	Banking (Account information)	PII	PCI (1)	HIPAA	FERPA	Business Confidential Data	Research (Most Secure)	Research (moderately secure)	Research (least secure)	Controlled, Unclassified Research Data (2)	ITAR Data (Export Control) (2)	IRB (Human Subject Research (3)	Intellectual Property (4)
Physical Security Requirements														
1. Doors														
a. Locked door	A	A	A	A	A	A	A	A	A	A				
b. Multifactor Identification/Access	A	A	A	A	A	A	A	A	S	N/A				
c. Enforced audit trail	A	A	A	A	A	A	A	A	N/A	N/A				
2. Audit tracking of access logs														
a. Sign-in and sign-out sheet	A	A	A	A	A	A	A	A	A	S				
b. Electronically tracked	A	A	A	A	A	A	A	A	S	N/A				
c. Records stored in separate, secure location	A	A	A	A	A	A	A	A	A	N/A				
3. Video security														
a. Unmonitored video recording w/out alerts (not useful for forensics)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A				
b. Unmonitored video recording w/ alerts	A	A	A	A	A	A	A	S	S	N/A				
c. Monitored video recording	N/A	N/A	N/A	N/A	N/A	N/A	N/A	S	S	N/A				
d. Recordings stored in separate, secure location	A	A	A	A	A	A	A	A	N/A	N/A				
4. Granting access to visitors (guests, vendors)														
a. Visitors must be signed in	A	A	A	A	A	A	A	A	A	S				
b. Visitors must be escorted/monitored at all times	A	A	A	A	A	A	A	A	S	S				
5. Alarms														
a. Door intrusion alarm-summon UNM-PD	A	A	A	A	A	A	A	A	N/A	N/A				
b. Door adjar/held open alarm-Relates to doors, access con	A	A	A	A	A	A	A	A	N/A	N/A				
6. Alarm response														
a. Police response	A	A	A	A	A	A	A	A	N/A	A				
b. Data Center Manager response	A	A	A	A	A	A	A	A	N/A	A				
c. Secondary contacts	A	A	A	A	A	A	A	A	N/A	A				
7. Contingency / Management Plan														
a. Physical Security plan (as a subset of recommended data custodian's DR/Incident Response Plan)	A	A	A	A	A	A	A	A	A	A				

(1) PCI security rules are frequently updated and can be found at https://www.pcisecuritystandards.org. UNM servers storing PCI data must also be approved by the UNM Controller and CIO.
(2) Classified research may not be conducted on a UNM campus. Controlled unclassified information must comply with NIST Special Publication 800-171 and must be approved and coordinated through the OVPR. All export controlled and Internaltional Traffic in Arms Regulations (ITAR) and EAR information require a Technology Control Plan from the Export Control Office of OVPR and be conducted in compliance with OVPR at UNM.
(3) Pending submission of content from the IRB.
(4) Pending submission of content from STC.

Appendix C
Glossary of Terms

Payment Card Industry (PCI) – Data Security Standard Glossary – https://www.pcisecuritystandards.org/security_standards/glossary.php

SANS Glossary of Security Terms - http://www.sans.org/security-resources/glossary-of-terms/?pass=f

Healthcare Insurance Portability and Accountability Act (HIPAA) Glossary of Terms – http://www.onlinetech.com/resources/references/hipaa-glossary-of-terms

Data Governance Glossary - http://www.datagovernance.com/glossary-governance/

Below **Compliance** Terms are from https://www.idology.com/resources/compliance-glossary-terms/

Gramm-Leach Bliley Act- This act requires financial institutions, companies that offer consumers financial products or services like loans, financial or investment advice, or insurance, to explain their information-sharing practices to their customers and to safeguard sensitive data.

Health Insurance Portability and Accountability Act (HIPAA) – The Health Insurance Portability and Accountability Act (HIPAA) is comprised of two parts. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Payment Card Industry (PCI) – Data Security Standard- The PCI data security standard is a set of guidelines that were developed by Visa, MasterCard, Discover and American Express to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. It is important for consumers to engage in a secure e-commerce, which is why the PCI data security standard was created.

Permissible Use – describes the intent of anyone accessing sensitive consumer data in that it must be for a legitimate business purpose. This prevents businesses from accessing information on people other than their customers.

Red Flag Regulations – Red Flag Regulations require financial institutions and creditors to develop and implement written identity theft prevention program. These programs must identify and detect the relevant warning signs or “red flags” of identity theft such as unusual account activity, fraud alerts on consumer report or attempted use of suspicious account application documents. There must also be appropriate responses that are described to prevent and resolve the crime and a plan to update the program.

Business Confidential Data: All information, unless categorized as Encrypted (E Class) or Public (P Class), used to support and conduct UNM Financial Services Division processes and business. Examples include but are not limited to:

- Payroll file (both paper and electronic) excluding those items listed in HIPAA Privacy Rule, IRS and other Federal or State bound restrictions
- Employment transactions
- Research Proposals
- Work in Progress Budgets
- PCard Number
- Address

Impacted Person: An individual or composite of individuals that are in some capacity hindered from accomplishing their mission critical functions on behalf of the university

Intellectual property data refers to data that is associated with creative works, ideas or inventions, including but not limited to the conduct of scholarly research, "embodied in a form than can be shared or can enable others to recreate, emulate, or manufacture". [Kulakowski & Chronister, 2006]. It includes but is not limited to data protected by patent, trademark, trade secrets, or copyright. Intellectual property may be a subset of Research Data or may exist outside of research, such as software.

Life Safety Code 101: Per wikipedia: "is a consensus standard widely adopted in the United States. It is administered, trademarked, copyrighted, and published by the National Fire Protection Association and, like many NFPA documents, is systematically revised on a three-year cycle. Despite its title, the standard is not a legal code, is not published as an instrument of law, and has no statutory authority in its own right. However, it is deliberately crafted with language suitable for mandatory application to facilitate adoption into law by those empowered to do so. The bulk of the standard addresses "those construction, protection, and occupancy features necessary to minimize danger to life from the effects of fire, including smoke, heat, and toxic gases created during a fire." The standard does not address the "general fire prevention or building construction features that are normally a function of fire prevention codes and building codes." http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=101

Mission Critical/Essential: Core components utilized in accomplishing the overall goal or missions(s) of the university and its units, departments, colleges, and institutes. Data or services whose failure, disruption or unavailability can or will cause failure in the business operation of an area. This can be measured by the degree of desired uptime and level of impact resulting from service unavailability.

Research Data refers to data generated and recorded using human, mechanical, electronic, or computational resources, or obtained from external sources as part of the conduct of a larger project, and which may be stored on a computer in the course of conducting scholarly or apprenticed (education and training) research. It "records the necessary data to construct and evaluate reported results, and the events and processes leading to research results" [Kulakowski & Chronister, 2006]. The data may originate in written, digital, or other media formats. It includes, **but is not limited to**, scholarly writings, measurements from recording instruments or sensor devices, computer code, data generated by computer programs, databases, or online searches, laboratory notebooks, technical documentation, technical notes, and covariate data associated with human subjects studies (HIPAA-protected data). The research itself may or may not be funded, and may or may not ultimately lead to publications or the filing of intellectual property rights.

Personally Identifiable Information (PII) or Sensitive Personal Information (SPI): Term used in US privacy law and information security. Any data that, when used on its own or with other information, could potentially identify, contact or locate a specific individual in context. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. This includes any information used to trace an individual's identity, such as name, social security number, data and place of birth, mother's maden name, or biometric records. This also includes other information that is linked or linkable to an individual, such as medical, educational, financial and employment infoermation. [GAO Report 08-536, 2008].

UNM Human Resources Information Data Classifications (Defined May 2015)

- **Confidential (E Class) Information – for data which must be encrypted**
  Information that has been determined by UNM Human Resources Information Stewards to require the highest level of privacy and security controls. Currently, any information that contains individually identifiable health information (one or more of the eighteen (18) identifiers found in the HIPAA Privacy Rule, that can be used to identify an individual that was created, used, or disclosed in the course of providing health care service), is considered to be Confidential (E Class) information. Additionally, the following data elements are considered to be Confidential (E Class) information if maintained for any reason
    - Protected Health Information
    - Benefits File (both paper and electronic)
    - Social Security Number
- **Restricted (C Class Information – for data which must be kept confidential**
  All information, unless categorized as Confidential (E Class) or Unrestricted
  (P Class), used to conduct UNM Human Resources business. Examples include but are not limited to:
    - Personnel file (both paper and electronic)
    - Employment transactions
- **Unrestricted (P Class) Information – for data which may be released to the public**
  Information that UNM Human Resources has made available or published for the explicit use of the general public. Examples include but are not limited to:
    - Sunshine Portal
    - Human Resources website

UNM Financial Services Data Classifications (Defined May,2015)

- **Confidential (E Class) Information – for which data must be encrypted**
  Information that has been determined by UNM Financial Services Division Information Stewards to require the highest level of privacy and security controls. Currently any information that contains protected individuall-identifiable information that can be used to identify or be associated to an individual is considered to be encrypted (E Class) informaiton. Additionally, the following data elements are considered to be E Class information if maintained for any reason:
    - Protected payroll and health benefits deduction information
    - Payroll file (paper and electronic), subject to potential HIPAA Privacy Rule, IRS and other Fedderal or State-bound restrictions (Garnishments)
    - Social Seuciryt Number
    - Banking Information
    - Tax Information
- **Confidential (C Class) Information – for data which must be kept confidential.**

All information, unless categorized as Encrypted (E Class) or Public (P Class), used to support and conduct UNM Financial Services Division processes and business. Examples include but are not limited to:

  - Payroll file (both paper and electronic) excluding those items listed in HIPAA Privacy Rule, IRS and other Federal or State bound restrictions
  - Employment transactions
  - Research Proposals
  - Work in Progress Budgets
  - PCard Number
  - Address

- **Public (P Class) Information - for data which may be released to the public**
  Information that Financial Services has made available or published for the explicit use of the general public. Examples include but are not limited to:
  - Records accessible pursuant to the NM Inspection of Public Records Act
  - Sunshine Portal
  - Various Financial Services Division websites

Uptime is a computer industry term for the time during which a computer is operational – working and available for use. Downtime is the time when it isn't operational. Uptime is sometimes measured in terms of a percentile. For example, one standard for uptime that is sometimes discussed is a goal called five 9s - that is, a computer that is operational 99.999 percent of the time. This equates to 5.39 minutes of totat downtime – planned or unplanned – in a given year.

References

Kulakowski, E. C., & Chronister, L. U. (2006). Research Administration and Management. London: Jones and Bartlett Publishers International.

GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, Government Accountability Office, May 2008, http://www.gao.gov/new.items/d08536.pdf.