Table of Contents

1. Purpose

Information is an important assets and must be protected from loss of integrity, confidentiality, or availability in compliance with policy and guidelines and state and federal laws and regulations.

2. Scope

This policy applies to all personnel that use organization information to create, access, store, or manage data to perform their business functions. It also applies to any third party vendor creating, storing, or maintaining data per a contractual agreement.

3. Policy

Data must be classified according to the Data Classification Schema and protected according to Data Security Standards. This policy applies to data in all formats or media.

3.1. Data Classification Schema

Information and the related data elements are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify Data based on its use, sensitivity to unauthorized disclosure, and requirements imposed by external entities.

Data elements are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. The classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

Data Classifications:

- ***Public*** - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the department, affiliates, or individuals. Public data generally have a very low sensitivity since it is general available, however some level of protection is warranted as data integrity can be important. Examples include:
  - Directory information for staff except for those who have requested non-disclosure
  - Records accessible pursuant to the NM Inspection of Public Records Act
  - Information on publicly accessible state web sites; example Sunshine Portal
  - Press releases

B. ***Internal*** - Data intended for internal business use only with access restricted to a specific division, group of individuals, or affiliates with a legitimate need to know. Internal data are generally not made available to parties outside of the department. Unauthorized disclosure could adversely impact the department or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

- Financial accounting data that does not contain confidential information
- Payroll file excluding those items listed in HIPAA Privacy Rule, IRS and other Federal or State bound restrictions
- Information technology transaction logs
- Employee ID numbers
- Employee addresses and phone numbers
- Directory information for staff who have requested non-disclosure

C. ***Restricted*** - Highly sensitive data intended for limited, specific use by a division or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the department or their affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or contracts. Restricted data have a very high level of sensitivity. Examples include:

- Social Security Number
- Law Enforcement records
- Personal identity information (PII). PII defined as an individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: a) Social security number, b) driver's license number or state identification card number, or c) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.
- Personnel records
- Medical records
- Authentication tokens (e.g., personal digital certificates, passwords, biometric data)

3.2. Data Security Standards

The following table defines required safeguards for protecting data and data collections based on their classification.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	***Data Classification***		
	Public	***Internal***	***Restricted***
Access Controls	• No restriction for viewing • Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function	• Viewing and modification restricted to authorized individuals as needed for business-related roles • Data Steward or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access	• Viewing and modification restricted to authorized individuals as needed for business-related roles • Data Steward or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access • Confidentiality agreement required
Copying/Printing (applies to both paper and electronic forms)	• No restrictions	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals with a need to know • Data should not be left unattended on a printer	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement • Data should not be left unattended on a printer • Copies must be labeled "Restricted"

Network Security	• May reside on a public network • Protection with a firewall recommended • IDS/IPS protection recommended • Protection only with router ACLs acceptable	• Protection with a network firewall required • IDS/IPS protection required • Protection with router ACLs optional • Servers hosting the data should not be visible to entire Internet • May be in a shared network server subnet with a common firewall ruleset for the set of servers	• Protection with a network firewall using "default deny" ruleset required • IDS/IPS protection required • Protection with router ACLs optional • Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks • Must have a firewall ruleset dedicated to the system • The firewall ruleset should be reviewed periodically by an external auditor
System Security	• Must follow general best practices for system management and security • Host-based software firewall recommended	• Must follow Dept-specific and OS-specific best practices for system management and security • Host-based software firewall required • Host-based software IDS/IPS recommended	• Must follow Dept-specific and OS-specific best practices for system management and security • Host-based software firewall required • Host-based software IDS/IPS recommended

Virtual Environments	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Should not share the same virtual host environment with guest virtual servers of other security classifications	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Cannot share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	• System must be locked or logged out when unattended • Host-based software firewall recommended	• System must be locked or logged out when unattended • Hosted in a secure location required; a Secure Data Center is recommended	• System must be locked or logged out when unattended • Hosted in a Secure Data Center required • Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	• No restrictions	• Access restricted to local network or general Virtual Private Network (VPN) service • Remote access by third party for technical support limited to authenticated, temporary access via secure protocols over the Internet	• Restricted to local network or secure VPN group • Unsupervised remote access by third party for technical support not allowed • Two-factor authentication recommended

Data Storage	• Storage on a secure server recommended • Storage in a secure Data Center recommended	• Storage on a secure server recommended • Storage in a secure Data Center recommended • Should not store on an individual's workstation or a mobile device	• Storage on a secure server required • Storage in Secure Data Center required • Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption • Encryption on backup media required • AES Encryption required with 192-bit or longer key • Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	• No restrictions	• No requirements	• Encryption required (for example, via SSL or secure file transfer protocols) • Cannot transmit via e-mail unless encrypted and secured with a digital signature
Backup/Disaster Recovery	• Backups required; daily	• Daily backups required	• Daily backups required

	backups recommended	• Off-site storage recommended	• Off-site storage in a secure location required
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	• See "Data Retention and Disposal Policy" • Paper: no restrictions	• See "Data Retention and Disposal Policy"	• See "Data Retention and Disposal Policy"
Training	• General security awareness training recommended • System administration training recommended	• General security awareness training required • System administration training required • Data security training required	• General security awareness training required • System administration training required • All staff must pass a criminal background check • Data security training required • Applicable policy and regulation training required
Audit Schedule	• As needed	• As needed	• Annual

4. Definitions

A. *ACL* - Access Control List; a set of rules in a network device, such as a router, that controls access to segments of the network. A router with ACLs can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.
B. *Authentication* - Process of verifying one's digital identity. For example, when someone logs into Webmail, the password verifies that the person logging in is the owner of the email account. The verification process is called authentication.
C. *Authorization* - Granting access to resources only to those authorized to use them.
D. *Availability* - Ensures timely and reliable access to and use of information.
E. *Confidentiality* - Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
F. *Firewall* - A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.

G. *IDS* - Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.
H. *Integrity* - Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.
I. *IPS* - Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.
J. *Local Network* - Any segment of the data network physically located on the Manhattan or Salina campus with an IP address starting with 129.130.X.X or an un-routable private IP address (e.g., 10.X.X.X).
K. *Remote Access* - Accessing any local network from any physical location outside the Manhattan or Salina campus. This includes access from off campus using VPN service.
L. *Secure Data Center* - A facility managed by full-time IT professionals for hosting computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and network firewall protection.
M. *Secure Server* - a computer that provides services to other computers, applications, or users; is running a server operating system; and is hardened according to relevant security standards, industry best practices, and security policies.
N. *Sensitivity* - Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.
O. *VPN* - Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

5. Roles and Responsibilities

Everyone with any level of access to Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing department Data and Data Collections.

A. *Chief Data Steward* - Senior administrative officers responsible for overseeing all information resources (e.g., the Director or Cabinet Secretary).
B. *Data Steward* – Division chiefs or their designees with responsibility for overseeing a collection (set) of Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each Data collection, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant polices and security requirements for all data for which they have responsibility.

C. *Data Manager* - Individuals authorized by a Data Steward to provide operational management of a Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.

D. *Data Processor* - Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

E. *Data Viewer* - Anyone with the capacity to access department Data but is not authorized to enter, modify, or delete it.

F. *Chief Information Security Officer* - Provides advice and guidance on information and information technology security policies and standards.

G. *Internal Audit Office* - Performs audits for compliance with data classification and security policy and standards.

6. Related Laws, Regulations, or Policies

New Mexico Inspection of Public Record Act (IPRA) -
http://www.nmag.gov/uploads/files/Publications/ComplianceGuides/Inspection%20of%20Public%20Records%20Compliance%20Guide%202015.pdf