An IT Compliance Regulations Matrix for Information Security

Laws & Regulations*	Designate Responsibility Required or Recommended		Establish Information Security Program		Establish Policies & Procedures		Monitoring/Incident Handling/ Compliance		Recommend a Training/Awareness Program	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
FERPA	Governance Committee**		X		X		X		X Required	
HIPAA	Security Official and Privacy Official		X		X		X		X Required***	
GLBA	One or more employees		X		X		X		X	
Red Flags Rule	Employee		X		X		X		X	
FISMA	Committee or Employee		X		X		X		X	
PCI DSS	individual or team for information security responsibilities		X		X		X		X	
NM State Law	There is no information security state law that regulates safeguarding and data breach notification of PII – The State Information Security Policy can be used as a Best Practice Guide.									
NMSU										

Legends:

* - Most regulations have developed audit checklists (except FERPA, but is being developed) to determine compliance. These checklists will be used by the IT Compliance Officer in the future to do in-depth reviews and ongoing monitoring of these processes at NMSU.

** - This is the recommended practice through a Technical Brief Guidance document provided by the Institute of Education Sciences on "Managing Personally Identifiable Information in Electronic Student Education Records." The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. A "Data Security Checklist" and other guidance resources provided by PTAC will be used to evaluate current NMSU's practices as it relates to FERPA compliance and a corrective action plan will be developed to ensure compliance at the institutional level.

*** - HIPAA's Standard 164.308 (a)(5) – Under the Security Awareness and Training section states that covered entities must: *"Implement a security awareness and training program for all members of its workforce (including management)."* It further states that Security training for all new and existing members of the covered entity's workforce is required by the compliance date of the Security Rule. Overall, the "Audit Protocol Checklist" provided by the U.S. Department of Health & Human Services (HHS) will be used to assess current NMSU's practices vs. HIPAA compliance requirements.

New Mexico State University - ICT
IT Compliance Selected Best Practices Matrix for Information Security

Generally Accepted Best Practice	Designate Responsibility Required		Establish Information Security Program		Establish Policies & Procedures		Monitoring/Incident Handling/ Compliance		Training/Awareness Program	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
COBIT 5*	X		X		X		X		X	
ISO Standards**	X		X		X		X		X	
NIST***	X		X		X		X		X	
GAPP****	X		X		X		X		X	
SANS – 20 Critical Controls*****	X		X		X		X		X	
Best Practices for Managing Information Security******	X		X		X		X		X	
Governing for Enterprise Security*******	X		X		X		X		X	
ITIL********	X		X		X		X		X	
NMSU										

Legends:

* - Source ISACA - Control Objectives for Information and Related Technologies (COBIT 5) – A Business Framework for the Governance and Management of Enterprise IT
** - Source - International Organization for Standardization – ISO Standard 27001 & ISO Standard 27002 – Information Security
*** - Source National Institute of Standards and Technology (NIST) Pub 800-53v3 - the Federal Information Security Management Act (FISMA)
**** - Source American Institute of Certified Public Accountants – Generally Accepted Privacy Principles (GAPP)
***** - Source SANS (SysAdmin, Audit, Network, Security) Institute
****** - Source IT Policy Compliance Group
******* - Source Carnegie Mellon University, Software Engineering Institute, CERT®
******** - Source The Information Technology Infrastructure Library (ITIL), is a set of practices for IT service management that focuses on the needs of business.

Note: The above represent ONLY the core/main principles that would set a strong foundation for a successful information security program at NMSU. The successful implementation of a University-wide security program depends on successfully implementing/establishing the above management controls.

Information Technology Policy Framework

	ISO 27002	COBIT 5	EDUCAUSE	NIST Pub. 800-53v3	FERPA		HIPAA		GLBA		RFR		PCI		NMSU	
					Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
1	Information Security Policy	Information security policy	Security Policy	Program Management	X		X		X		X		X			
2	Organization of Information Security		Organization of Information Security		X		X		X		X		X			
3	Asset Management	Asset management policy	Asset Management		X		X		X		X		X			
4	Human Resources Security	Personnel information security policy	Human Resources Security	Personnel Security	X		X		X		X		X			
5	Physical and Environment Security	Physical and environmental information security policy	Physical and Environmental Security	Physical and Environment Procedures	X		X		X		X		X			
6	Communications and Operations	Communications and operation management policy	Communications and Operations	System and Communications Protection	X		X		X		X		X			
7	Accounts and Access Controls	Access control policy	Access Control	Access Control	X		X		X		X		X			
8	Systems Acquisition, Development, Maintenance	Information systems acquisition, software development and maintenance policy	Systems Acquisition, Development, Maintenance	System and Services Acquisition	X		X		X		X		X			
9	Security Incident Handling	Incident management policy	Information Security Incident Handling	Incident Response	X		X		X		X		X			
10	Business Continuity Management	Business continuity and disaster recovery policy	Business Continuity Management	Contingency Planning	X		X		X		X		X			
11	Compliance	Compliance policy	Compliance	Audit and Accountability	X		X		X		X		X			
12		Risk management policy	Risk Assessment	Risk Assessment	X		X		X		X		X			
13		Vendor management policy			X		X		X		X		X			
14		Rules of behavior (acceptable use)			X		X		X		X		X			
15				System and Information Integrity	X		X		X		X		X			
16				Planning	X		X		X		X		X			
17				Media Protection	X		X		X		X		X			
18				Maintenance	X		X		X		X		X			
19				Identification and Authentication	X		X		X		X		X			
20				Configuration Management	X		X		X		X		X			
21				Security Assessment and Authorization	X		X		X		X		X			
22				Awareness and Training	X		X		X		X		X			

Roadmap – 2 -5yrs to Implement

IT Security/Compliance Framework for Information Security in Higher Ed

	Designate Responsibility Required or Recommended*		Establish Information Security Program*		Establish Policies & Procedures*		Monitoring /Incident Handling/ Compliance**		Establish a Training/Awareness Program**	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
FERPA, HIPAA, GLBA, RFR, PCI DSS and Best Practices	X		X		X		X		X	
Methodology to Implement Framework	1. University-wide responsibility should be designated to an employee (CISO or similar). The CISO can report to the CIO with a dotted line to an Audit Committee or University Auditor. 2. Alternative, establish a University-wide IT Security Committee to govern IT Security. A CISO should be appointed to manage/implement program.		A risk-based information security program/plan should be developed considering the following: 1. Compliance with applicable laws & regulations. 2. Management needs. 3. Best Management Practices.		Develop Information Technology Policies. Refer to previous table for more details.		1. An incident handling policy and procedures should be developed to ensure data breaches/incidents are handled according to the applicable requirements. 2. A regular auditing/monitoring program should be established to ensure compliance with federal, state and industry regulations.		1. A mandatory computer & data security training should be implemented and all employees should be trained. 2. Highly specialized trainings should be developed and be customized for employees that handle regulated data (FERPA, HIPAA, etc.) depending on the applicable federal, state or industry regulation.	

Legend:

*** - Implement chronologically**

**** - Can be implemented as soon as possible**