COMPARES UAC 1st read to UAC 2nd read v081219

15.25 – IT Investigation v081219

PART 1: ~~PURPOSE~~RECOGNITION AND AUTHORIZATION FOR IT INVESTIGATIONS

A. ~~This rule recognizes, and provides guidance relating to, the investigative support function served by NMSU Information and Communications Technologies (ICT), referred to as "IT investigation". When authorized in accordance with this rule, IT investigations may access, duplicate, search, gather, organize and provide~~**Definition of IT Investigation**: An IT investigation consists of accessing, duplicating, searching, gathering, organizing and providing data from NMSU computer systems, user accounts and data repositories maintained on NMSU owned or controlled resources~~.~~ in response to a request from an authorized official's request in accordance with this rule.

~~PART 2: INQUIRIES OR ISSUES REQUIRING IT INVESTIGATION~~

B. ~~**Types of IT Investigations**: The most common IT investigations are: (1) internal NMSU investigations (e.g.~~ **Authority to Conduct IT Investigations**: This rule recognizes the authority of the Information Security (InfoSec) and Privacy/Compliance departments within NMSU Information and Communications Technologies (ICT), to conduct IT investigations in response to requests from authorized university officials, as their respective positions may require for official university business.

1. Unless a specific exception applies, all requests for IT investigative assistance and support must be made in accordance with this rule.

2. The routine gathering of digital data by the university's various NMSU data stewards (e.g. to respond to requests for inspection of public information or to respond to student requests under FERPA) is not considered an "IT Investigation". However, if a data steward requires investigative assistance from ICT, this rule will apply.

~~A. personnel, audit); (2) external requests for information determined to be legally required or necessary in the best interest of NMSU (e.g. requests for inspection of public records, subpoenas); and (3) operational, for continuity or security of NMSU business operations. If a request for IT investigation does not fall into one of these categories, ICT will seek approval from one or more of the NMSU officials listed below in Part 3 B. 3, and if approved, will proceed in accordance with this rule.~~

~~B. **Exclusions:** Not covered by this rule, and not considered to be "IT Investigation", is the routine gathering of university digital data by an NMSU data steward required for day to day operations, unless ICT resources are required to independently locate and produce records, in which case, this rule will apply. Examples of searches for data not considered IT investigation include a search by the designated records custodian for public or directory information in response to a request for inspection of public records, or a search by the registrar or designee to produce student educational records in response to the student's request, as required by FERPA.~~

~~PART 3: PROCEDURES~~

3. ~~**Authorization Required for IT Investigation:**~~ Individual departments are not authorized to conduct ~~an IT investigation.~~ IT investigations, as defined in this rule.

~~A.~~4. If an NMSU supervisor or employee believes ~~an~~ IT investigation ~~should be conducted~~is necessary to support their work, they must coordinate through their dean, vice president or equivalent authority not implicated in the allegations to contact the appropriate authority (See ~~B. 3~~Part 2 C. below) to ~~request an~~coordinate such IT investigation.

~~B. **Process for Internal NMSU Investigations**: When there is a reasonable suspicion that a law and/or university policy, rule or procedure has been violated, or when litigation is reasonably anticipated, the university's internal investigative response may involve a request for IT investigation.~~

~~1. A request for IT investigation in support of an internal NMSU investigation must be submitted solely to the chief information security officer (CISO) or designee.~~

~~2. Investigations made in reasonable anticipation of litigation should be referred to and will be directed by the chief legal affairs officer. This referral is the responsibility of ICT and/or the authorizing official.~~

~~3. Any of the following NMSU officials are authorized to request, in writing, an IT investigation relating to an internal NMSU investigation within the scope of their area of responsibility or jurisdiction. The official must provide the data gathering, confidentiality and delivery date requirements to ICT to commence the IT Investigation.~~

~~a.~~1.~~Chancellor~~
~~b.~~1.~~Campus Presidents~~
~~c.~~1.~~Executive Vice President and Provost~~
~~d. Chief Legal Affairs Officer~~
~~e.~~1.~~AVP HRS~~
~~f.~~1. ~~Dean of Students~~
~~g.~~1.~~Director of Office of Institutional Equity~~
~~h.~~1.~~Chief Audit Officer~~
~~i.~~1. ~~NMSU Police Chief~~
~~j. IT Compliance Officer~~

C. ~~**Process for Official External Requests for Information**: NMSU receives a variety of external requests for data stored in the university's IT records which may necessitate IT investigation.~~ **Types of IT Investigations**: ICT InfoSec and Privacy and Compliance departments regularly respond to official requests to conduct IT Investigation in support of the following three types of authorized university business. If a request does not fall into one of these categories, ICT InfoSec and/or Privacy and Compliance may seek additional clarification and approval from an authorized official before proceeding.

~~C.~~ NMSU internal investigations (e.g. personnel, audit); ~~To initiate IT investigation in support of an external request (e.g. IPRA, Subpoena or educational or research regulatory body), the following applies:~~

~~1. To determine the legitimacy of the external request and the university's obligation to respond, external requests involving access or production of records from IT data must be reviewed and approved by either the university's chief legal affairs officer or designee, and in the case of requests from outside law enforcement agencies, also the NMSU police chief or designee.~~

~~2. Valid external requests for IT investigation must be submitted solely to the chief information security officer (CISO) or designee.~~

~~D. **Process for IT Operational Investigations**: IT staff at NMSU frequently perform routine operational IT investigations relating to business continuity and security.~~

~~1. Operational IT investigations are initiated by IT staff, without the need for other authorization, but must be based on a reported or observed system failure, error, or performance anomaly or reasonable suspicion of a data breach, data loss, other compliance violation or possible harm to the institution exists (IT Incident).~~

1. ~~If not already involved in the investigation, IT staff must promptly notify the chief information officer (CIO) or chief information security officer (CISO) or IT compliance officer when~~

2. Legally required external requests for information (e.g. requests for inspection of public records, subpoenas); and

3. Operational, for continuity or security of NMSU business operations.

~~2.~~ **Integrity and** ~~an operational IT investigation determines that an IT Incident may have occurred, an employee, student or affiliate becomes the focus of the investigation, or it is likely that a crime has been committed.~~

~~E.~~D. **Performance of IT Investigation**: The ~~chief information security officer's~~CISO's designees ~~in Information & Communication Technologies (~~within ICT~~) Information Security (~~ InfoSec~~) department~~ and the ~~information technology compliance officer~~IT Privacy and Compliance Officer will conduct approved IT investigations. To preserve the integrity of an IT investigation, the maintenance of strict confidence is required by all persons involved in conducting or performing the IT investigation. Violations of confidentiality will be referred to HR and Legal Counsel for resolution.

1. In the course of conducting IT Investigation, ICT may contract the services of a security vendor.

2. ~~ICT~~IT investigators may task investigative duties to other IT staff both internal and external to ICT in order to facilitate the gathering of digital data to meet the requirements of the IT investigation and data protection requirements.

3. ICT investigators are not required to disclose the purpose of the request for data to individuals tasked with assisting in the data collection or to ~~otherwise~~others required to cooperate with the investigation~~, beyond stating "An official NMSU investigation requires your cooperation."~~. IT investigators will provide the identity of the official who authorized the IT investigation to those who seek verification of the official nature of the IT investigation.

4. All IT investigators are required to follow the data protection requirements mandated by the type of regulated digital data being viewed or collected for an investigation and are not required to inform the data owner or data steward that the data is being accessed.

5. IT Investigations ~~that are determined~~may indicate or confirm an IT Incident subject to ~~be a compliance violation (IT incident), may have~~corresponding contractual or reporting requirements~~. The~~; the IT compliance officer will ~~make this determination.~~determine the specific reporting requirements and coordinate with appropriate university administrators through the CIO.

6. Discovery of lawful digital data, violating NMSU policy, but not material to the approved investigation, will be reported to the chief legal affairs officer for review.

7. If an IT investigation results in the suspicion or discovery of child pornography, the investigator must immediately halt the investigation and contact the NMSU police department.

PART 2: IT INVESTIGATION SUPPORTING NMSU INTERNAL INVESTIGATIONS

When there is a reasonable suspicion that a law and/or university policy, rule or procedure has been violated (e.g. internal HR or Internal Audit investigation), or when litigation is reasonably anticipated, the university's internal investigative response may involve a request for IT investigation.

A. **Notice to CISO**: A request for IT investigation in support of an internal NMSU investigation must be directed to ICT InfoSec's chief information security officer (CISO).

B. **Notice to Chief Legal Affairs Officer**: Authorizing officials must refer to the chief legal affairs officer requests for investigation pertaining to matters that involve reasonably anticipated litigation.

C. **NMSU Officials Authorized to Request IT Investigation**: The following officials may request an IT investigation relating to an internal NMSU investigation within the scope of their area of responsibility or jurisdiction by submitting a written request to the CISO or designee. The requesting official must provide the constraints relating to the data requested, as well as confidentiality and delivery date requirements, after which ICT will commence the IT Investigation.

1. Chancellor
2. Campus Presidents

3. Executive Vice President and Provost
4. Chief Legal Affairs Officer and UGC attorneys
5. AVP HRS
6. Dean of Students
7. Director of Office of Institutional Equity
8. Chief Audit Officer
9. NMSU Police Chief
10. IT Compliance Officer

PART 3: IT INVESTIGATION SUPPORTING EXTERNAL REQUESTS

NMSU receives a variety of external requests for data stored in the university's IT records which may necessitate IT investigation. IT investigation in support of external requests made to the various departments will be initiated after validation of the request, and assignment by the CISO.

A. **Validation of Request:** NMSU Chief Legal Affairs Officer, in consultation with NMSU Police Chief in matters involving outside law enforcement agencies, determines the legitimacy of all external requests involving access or production of records from IT data.

B. **Assignment by CISO**: Valid external requests for IT investigation must be directed to ICT InfoSec's Chief Information Security Officer (CISO) for review and assignment to a designee within ICT InfoSec or Privacy and Compliance designee.

PART 4: IT INVESTIGATION FOR NMSU BUSINESS CONTINUITY AND SECURITY

Information Technology staff throughout the NMSU system perform routine operational functions which relate to business continuity and security and which are subject to this rule.

A. **Initiation of IT Investigation**: Operational IT investigations are initiated by IT staff, without the need for other authorization, but must be based on a reported or observed system failure, error, or performance anomaly or reasonable suspicion of a data breach, data loss, other compliance violation or possible harm to the institution exists, any of which would constitute an IT Incident.

B. **Notification to ICT CIO, CISO or IT Compliance Officer**: IT staff must promptly notify the chief information officer (CIO), CISO or IT compliance officer when:

1. an operational IT investigation determines that an IT Incident may have occurred,
2. an employee, student or affiliate becomes the focus of the investigation, or
3. it is suspected that a crime has been committed.

~~7.~~