NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

Interim Information Security & Privacy Policy

Interim policy

Last Updated:
June 23, 2023

Responsible Department:
Information Technology & Communications

Policy Purpose: Establish guidelines for data custodians and stewards to responsibly manage data in accordance with NMT needs & requirements.

Table of Contents

Policy Statement

New Mexico Tech (NMT) requires all who have access to and/or responsibilities for data to manage it as set forth in this policy.

This requirement is to be in accordance with the rules regarding collection, storage, disclosure, access, processing, destruction, classification of information, and Privacy & Security Standards.

Purpose of Policy

New Mexico Tech must maintain and protect its informational assets and comply with applicable international, federal, state laws and contractual agreements.

To meet this stated objective, this policy document has been created and serves as the Written Information Security Program (WISP) document.

Who Should Read This Policy

All employees with access to and/or responsibilities for data should read this policy.

Who is Affected by This Policy?

All departments and organizations of NMT and all employees of NMT must adhere to this policy.

Most Current Version of This Policy

The most current version of this policy can be obtained from the NMT website. https://www.nmt.edu/policies/

Contacts

Consult with your division head and/or unit director for general questions about this policy. For specific policy issues use the following contact information:

Subject	Contact	Telephone	Email
Policy Clarification & All other issues	Information Security Group	(575) 835-5700	itciso@nmt.edu

Department/Unit Procedure Provision Documents

The various procedures to be written and implemented by NMT and/or NMT's departments or units as specified by this policy shall be named in the following manner and correspond to specific procedures as outlined in this policy document under the **Department/Unit Procedure Provisions & Policy List** section.

Entity	Procedure	Department / Unit	Procedure Number
NMT	.(GOV, AST, BCD, ...)	.(NMT, ITC, Budget, ICASA...)	.001

For example, a Governance (GOV) Procedure can be referred to as NMT.GOV.NMT.001 for a NMT base procedure and NMT.GOV.ITC.001 for a department specific procedure.

The procedure documents will contain sections specifying which specific departments and/or units they are applicable. The version of the procedure and dates showing when it was approved and last modified. Lastly, procedures will have a section showing the appropriate approving authority, as applicable.

Department/Organization Procedure Provisions & Policy List

NMT.GOV	Governance (GOV) Procedure Provision
NMT.AST	Asset Management (AST) Procedure Provision
NMT.BCD	Business Continuity & Disaster Recovery (BCD) Procedure Provision
NMT.END	Endpoint Security (END) Procedure Provision
NMT.MDM	Mobile Device Management (MDM) Procedure Provision
NMT.IRH	Incident Response & Handling (IRH) Procedure Provision
NMT.CHG	Change Management (CHG) Procedure Provision
NMT.CFG	Configuration Management (CFG) Procedure Provision
NMT.CRY	Cryptographic Protections (CRY) Procedure Provision
NMT.DCH	Data Classification & Handling (DCH) Procedure Provision
NMT.HRS	Human Resources Security (HRS) Policy
NMT.IAC	Identification & Authentication (IAC) Procedure Provision
NMT.IAP	Information Assurance (IAP) Procedure Provision
NMT.PRI	Privacy (PRI) Procedure Provision
NMT.RSK	Risk Management (RSK) Policy
NMT.SOS	Security Operations (SOS) Policy
NMT.TPM	Third-Party Management (TPM) Procedure Provision
NMT.CLD	Cloud and Web Security (CLD) Procedure Provision
NMT.SLP	Cyber Literacy Program (SLP) Procedure Provision
NMT.THR	Threat Management (THR) Procedure Provision
NMT.VFM	Vulnerability & Flaw Management (VFM) Procedure Provision
NMT.SDL	Secure Development Life Cycle (SDL) Procedure Provision
NMT.TDA	Technology Development & Acquisition (TDA) Procedure Provision
NMT.SEA	Secure Engineering & Architecture (SEA) Procedure Provision
NMT.NET	Network Security (NET) Procedure Provision
NMT.PES	Physical & Environmental Security (PES) Procedure Provision
NMT.MON	Continuous Monitoring Security (MON) Procedure Provision
NMT.CPL	Compliance (CPL) Procedure Provision

Department/Unit Procedure Provisions Policy Details

NMT.GOV Governance (GOV) Procedure Provision

Purpose:

The Security & Privacy Governance (GOV) Procedure Provision is to specify the development, proactive management, and ongoing review procedures of NMT departments & units.

Policy:

NMT and/or NMT departments & Units shall create written Security & Privacy Governance (GOV) procedure(s) to protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored.

Information privacy and security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and systems, in accordance with the applicable statutory, regulatory and contractual obligations.

These written procedure(s) shall be implemented by NMT departments & Units.

NMT.GOV Governance (GOV) Procedure

NMT.AST Asset Management (AST) Procedure Provision

Purpose:

The Asset Management (AST) Procedure Provision is to ensure that technology assets are properly managed throughout the life cycle of the asset, from procurement through disposal.

Policy:

NMT and/or NMT departments & units shall create written Asset Management (AST) procedure(s) which will protect assets and associated data throughout its life cycle from procurement through the disposal process.

These written procedure(s) shall be implemented by NMT departments & units.

NMT.AST Asset Management (AST) Procedure

NMT.BCD Business Continuity & Disaster Recovery (BCD) Procedure Provision

Purpose:

The Business Continuity & Disaster Recovery (BCD) Procedure Provision is to establish procedures that will help NMT recover from adverse situations with minimal impact on operations.

Policy:

NMT departments & units shall create written Business Continuity & Disaster Recovery (BCD) procedure(s) for their critical data & processes to ensure the availability of critical technology resources during adverse conditions.

These written procedure(s) shall be incorporated into the NMT disaster recovery plan.

The created procedure(s) shall be reviewed, tested, and updated as needed, on an annual basis by the NMT departments & units and as part of the NMT disaster recovery plan testing and validation process.

NMT.BCD.001	Business Continuity & Disaster Recovery (BCD) Procedure

NMT.END Endpoint Security (END) Procedure Provision

Purpose:

The purpose of the Endpoint Security (END) Procedure Provision is to ensure that endpoint devices are appropriately protected from reasonable threats.

Applicable statutory, regulatory, and contractual obligations will dictate the safeguards that must be in place to protect the technology & data assets.

Policy:

NMT and/or NMT departments & units shall create written Endpoint Security (END) procedure(s) to protect endpoints from reasonable threats and meet the applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by NMT departments & units.

NMT.END	Endpoint Security (END) Procedure

NMT.MDM Mobile Device Management (MDM) Procedure Provision

Purpose:

The Mobile Device Management (MDM) Procedure Provision is to identify & establish security measures that should be adopted to appropriately manage the risks to NMT technology & data assets introduced by using mobile devices, regardless if the device is owned by NMT, its users or trusted third-parties.

Policy:

NMT and/or NMT departments & units shall create written Mobile Device Management (MDM) procedure(s) to appropriately manage the risks to NMT technology & data assets associated with mobile device use and meet the applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.MDM Mobile Device Management (MDM) Procedure

NMT.IRH Incident Response & Handling (IRH) Procedure Provision

Purpose:

The purpose of the Incident Response & Handling (IRH) Procedure Provision is to incorporate NMT departments & units specific procedures into the NMT Incident Response & Handling plan to address and manage security-related incidents when they occur.

Policy:

NMT departments & units shall create written Incident Response & Handling (IRH) procedure(s) that addresses the specific technology & data assets concerns per applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be incorporated into the NMT Incident Response & Handling Plan.

NMT.IRH Incident Response & Handling (IRH) Procedure

NMT.CHG Change Management (CHG) Procedure Provision

Purpose:

The Change Management (CHG) Procedure Provision is to proactively manage change.

Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the institution.

Policy:

NMT and/or NMT departments & units shall create written Change Management (CHG) procedure(s) that follows a standard process to reduce the risk associated with change.

These procedure(s) shall include the appropriate provisions to ensure changes are appropriately tested, validated and documented before implementing any change on a production technology asset.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.CHG Change Management (CHG) Procedure

NMT.CFG Configuration Management (CFG) Procedure Provision

Purpose:

The purpose of the Configuration Management (CFG) Procedure Provision is to establish and maintain the integrity of technology assets.

Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.

Policy:

NMT and/or NMT departments & units shall create written Configuration Management (CFG) procedure(s). These procedure(s) may be a part of the written Change Management (CHG) procedure NMT.CHG.

These procedures shall apply to all technology assets used in production NMT business operations.

These procedures shall include provisions for accurate inventories of technology platforms. Provisions to define security standards for the technology platforms shall be included. Provisions for the annual review and validation of these security settings shall be included.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.CFG Configuration Management (CFG) Procedure

NMT.CRY Cryptographic Protections (CRY) Procedure Provision

Purpose:

The purpose of the Cryptographic Protections (CRY) Procedure Provision is to protect the confidentiality of data by implementing appropriate cryptographic technologies to protect data assets while also minimizing the inadvertent loss of access to data assets.

Policy:

NMT and/or NMT departments & units shall create written Cryptographic Protections (CRY) procedure(s) to apply appropriate cryptographic safeguards to protect data assets against loss, unauthorized access or disclosure. These procedure(s) shall apply to data, regardless if it is at rest or in transit.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.CRY Cryptographic Protections (CRY) Procedure

NMT.DCH Data Classification & Handling (DCH) Procedure Provision

Purpose:

The purpose of the Data Classification & Handling (DCH) Procedure Provision is to ensure that technology & data assets are properly classified and measures are implemented to protect data from unauthorized disclosure, regardless if data is being transmitted or stored.

Applicable statutory, regulatory and contractual obligations dictate the safeguards that must be in place to protect the confidentiality, integrity and availability of data.

Policy:

NMT and/or NMT departments & units shall create written Data Classification & Handling (DCH) procedure(s) which shall protect data by limiting access to authorized users and utilize methods of sanitizing or destroying media so that data recovery is technically infeasible as required by applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.DCH Data Classification & Handling (DCH) Procedure

NMT.HRS Human Resources Security (HRS) Policy

Purpose:

The purpose of the Human Resources Security (HRS) Policy is to create a security-minded workforce and an environment.

Policy:

NMT shall ensure appropriate practices for cybersecurity are incorporated into Human Resources (HR) personnel management practices

NMT.HRS Human Resources Security (HRS) Policy

NMT.IAC Identification & Authentication (IAC) Procedure Provision

Purpose:

The purpose of the Identification & Authentication (IAC) Procedure Provision is to ensure authorized devices and users are properly identified and authenticated to gain access to NMT technology & data assets. The appropriate identification & authentication will be used for proper compliance with applicable statutory, regulatory and contractual obligations.

Policy:

NMT and/or NMT departments & units shall create written Identification & Authentication (IAC) procedure(s) which shall protect NMT technology & data assets by implementing necessary identification & authentication mechanisms in compliance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.IAC Identification & Authentication (IAC) Procedure

NMT.IAP Information Assurance (IAP) Procedure Provision

Purpose:

The purpose of the Information Assurance (IA) Procedure Provision is to ensure reasonable assurance is used in the development, implementation, assessment, authorization and monitoring of the security program.

Policy:

NMT and/or NMT departments & units shall create written Information Assurance (IA) procedure(s) which shall conduct periodic assessments of NMT technology & data assets to evaluate the effectiveness of applicable security controls.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.IAP Information Assurance (IAP) Procedure

NMT.PRI Privacy (PRI) Procedure Provision

Purpose:

The purpose of the Privacy (PRI) Procedure Provision is to ensure appropriate safeguards are implemented to protect Personal Information (PI) in accordance with applicable statutory, regulatory, and contractual obligations.

Policy:

NMT and/or NMT departments & units shall create written Privacy (PRI) procedure(s) defining appropriate security controls to protect Personal Information (PI) in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.PRI Privacy (PRI) Procedure

NMT.RSK Risk Management (RSK) Policy

Purpose:

The purpose of the Risk Management (RSK) Policy is to ensure that cybersecurity-related risk is visible and understood.

Policy:

NMT and/or NMT departments & units shall periodically assess and document the risk to business operations and technology & data assets which are associated with processing, storage, or transmission of information supporting NMT business processes.

The assessment and documentation shall include information & sources, NMT evaluation, and actions taken in regard to these risks.

NMT.RSK Risk Management (RSK) Policy

NMT.SOS Security Operations (SOS) Policy

Purpose:

The purpose of the Security Operations (SOS) Policy is to address the service delivery of cybersecurity operations.

Policy:

NMT departments & units with cybersecurity operations shall be staffed by appropriately qualified personnel to provide the protective, detective and response services to support the NMT security programs.

NMT.SOS Security Operations (SOS) Policy

NMT.TPM Third-Party Management (TPM) Procedure Provision

Purpose:

NMT must assess the cybersecurity and privacy risks posed by both its current and potential third-party providers.

To be in compliance with applicable statutory, regulatory and contractual obligations, third-parties to NMT must implement mechanisms to identify and remediate deficiencies and/or vulnerabilities on an ongoing basis.

Policy:

NMT and/or NMT departments & units shall create written Third-Party Management (TPM) procedure(s) which will validate that current and potential third-party providers have mechanisms to identify and remediate deficiencies and/or vulnerabilities. These procedure(s) shall perform this validation at least on an annual basis.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.TPM Third-Party Management (TPM) Procedure

NMT.CLD Cloud and Web Security (CLD) Procedure Provision

Purpose:

The purpose of the Cloud Security (CLD) Procedure Provision is to govern the use of private and public cloud environments (e.g., IaaS, PaaS and SaaS) to manage risks associated with third-party involvement and architectural decisions.

Policy:

NMT and/or NMT departments & units shall create written Cloud Security (CLD) procedure(s) which shall manage risk in all of its cloud environments in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.CLD	Cloud and Web Security (CLD) Procedure

NMT.SLP Security Literacy Program (SLP) Procedure Provision

Purpose:

The purpose of the Security Literacy Program (SLP) Procedure Provision is to develop a security and privacy-minded workforce.

Policy:

NMT and/or NMT departments & units shall create written Security Literacy Program (SLP) procedure(s) which shall ensure that users are made aware of the security and privacy risks associated with their roles and that users understand the applicable statutory, regulatory and contractual compliance requirements related to the security and privacy of systems and data within their sphere of influence.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.SLP	Cyber Literacy Program (SLP) Procedure

NMT.THR Threat Management (THR) Procedure Provision

Purpose:

The purpose of the Threat Management (THR) Procedure Provision is to establish a capability to proactively govern technology-related threats to the privacy & security of NMT's systems, data and business processes.

Policy:

NMT and/or NMT departments & units shall create written Threat Management (THR) procedure(s) which shall implement the capability to proactively govern threats which shall include but is not limited to the identification, assessment and remediation of threats to NMT's systems, data and business processes in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.THR	Threat Management (THR) Procedure

NMT.VFM Vulnerability & Flaw Management (VFM) Procedure Provision

Purpose:

The purpose of the Vulnerability & Flaw Management (VFM) Procedure Provision is to manage the risks associated with technical vulnerabilities.

Policy:

NMT and/or NMT departments & units shall create written Vulnerability & Flaw Management (VFM) procedure(s) which shall manage vulnerabilities both in how its technology assets are configured and the level of currency in software patching in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.VFM	Vulnerability & Flaw Management (VFM) Procedure

NMT.SDL Secure Development Life Cycle (SDLC) Procedure Provision

Purpose:

The purpose of the Secure Development Life Cycle (SDLC) Procedure Provision is to protect against avoidable impacts to operations by managing critical technology assets and supporting infrastructure during program, system, and software life cycles.

Policy:

NMT and/or NMT departments & units will create written Secure Development Life Cycle (SDLC) procedure(s) to identify technology & data assets which are critical to NMT business operations.

These procedure(s) shall define appropriate security measures during all phases of the life cycle of identified technology & data assets to minimize security and privacy-related risks in accordance with applicable statutory, regulatory, and contractual obligations.

These written procedure(s) shall be implemented by NMT departments & units.

NMT.SDL	Secure Development Lifecycle (SDL) Procedure

NMT.NET Network Security (NET) Procedure Provision

Purpose:

The purpose of the Network Security (NET) Procedure Provision is to ensure sufficient security controls are in place to protect the confidentiality and integrity of NMT's communications, as well as to provide situational awareness of activity on NMT's networks.

Policy:

NMT and/or NMT departments & units shall create written Network Security (NET) procedure(s) which shall govern security mechanisms to keep its networks secure from evolving threats, while providing situational awareness of network activities so that proactive measures can be implemented to address evolving threats.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.NET Network Security (NET) Procedure

NMT.PES.001 Physical & Environmental Security (PES) Procedure Provision

Purpose:

The purpose of the Physical & Environmental Security (PES) Procedure Provision is to minimize risk to NMT's technology & data assets by addressing applicable physical security and environmental concerns.

Policy:

NMT and/or NMT departments & units shall create written Physical & Environmental Security (PES) procedure(s) which shall implement appropriate physical access controls to limit access to systems, equipment and the respective operating environments to authorized individuals.

These procedure(s) shall provide for appropriate environmental controls in facilities containing systems to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.PES Physical & Environmental Security (PES) Procedure

NMT.MON Continuous Monitoring (MON) Procedure Provision

Purpose:

The purpose of the Continuous Monitoring (MON) Procedure Provision is to establish and maintain awareness across the institution through the centralized collection and review of security-related event logs.

Policy:

NMT and/or NMT departments & units shall create written Continuous Monitoring (MON) procedure(s) which shall establish a configuration management requirement for applicable technology assets to log security events and forward those events to allow for monitoring and review of logs in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.MON Continuous Monitoring Security (MON) Procedure

NMT.CPL Compliance (CPL) Procedure Provision

Purpose:

The purpose of the Compliance (CPL) Procedure Provision is to verify safeguards are in place to document compliance with applicable statutory, regulatory and contractual obligations.

Policy:

NMT and/or NMT departments & units shall create written Compliance (CPL) procedure(s) which shall define appropriate safeguards to protect sensitive business data against loss, unauthorized access or disclosure in accordance with applicable statutory, regulatory, and contractual obligations.

These procedure(s) shall be implemented by the NMT departments & units.

NMT.CPL	Compliance (CPL) Procedure

Document Change Record

REVISION NUMBER	DESCRIPTION OF CHANGE	CHANGED PAGE(S)	DATE	AUTHOR
0.01	Initial Draft	All	2023.01.15	Dan Lunceford
1.00	Draft	All	2023.04.03	Dan Lunceford
1.10	Compass vISO Draft	All	2023.05.11	Compass ITC
1.50	Adjusted for NMT	All	2023.06.05	Morey Roof
1.60	Working Group Changes	All	2023.06.12	Morey Roof
1.70	Working Group Changes	All	2023.06.13	Morey Roof
1.80	Font changes	All	2023.06.15	Chris Knight
1.90	Formatting Changes	All	2023.06.19	Daniel Lunceford
2.0	Incorporating AVP AF Comments	All	2023.06.23	Daniel Lunceford
2.1	Added Signature Page	Last	2023.06.23	Daniel Lunceford

Violations

Any NMT personnel found to have violated the policy and/or procedure may be subject to appropriate disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

While every exception potentially weakens protection mechanisms for NMT systems and underlying data, occasionally exceptions will exist. When requesting an exception, the requestor is required to submit a business justification and the exceptions will be documented in the procedures.

References

This is a non-exhaustive list of references which are the source standards and resources used to create and support this document.

NMT Information Privacy and Security recognizes two sources for authoritative definitions:

- The National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Privacy and Security Terms*, is the approved reference document used to define common cybersecurity terms.
- Unified Compliance Framework (UCF) Compliance Library.

The following external content is a non-exhaustive list of frameworks that are referenced by or support this Information Security and Privacy Policy:

- The National Institute of Standards and Technology (NIST):
    - NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST 800-39: Managing Cybersecurity Risk: Organization, Mission and Information System View
    - NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
    - NIST 800-64: Security Considerations in Secure Development Life Cycle
    - NIST 800-122: Guide to Protecting the Confidentiality of Personal Information (PI)
    - NIST 800-160: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
    - NIST 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
    - NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
    - NIST IR 7298: Glossary of Key Cybersecurity Terms
    - NIST IR 8179: Criticality Analysis Process Model: Prioritizing Systems and Components [draft]
    - NIST Framework for Improving Critical Cybersecurity (Cybersecurity Framework)

- The International Organization for Standardization (ISO):
  - ISO 15288: Systems and Software Engineering -- System Life Cycle Processes
  - ISO 22301: Societal Security – Business Continuity Management Systems – Requirements
  - ISO 27002: Information Technology -- Security Techniques -- Code of Practice for Cybersecurity Controls
  - ISO 27018: Information Technology -- Security Techniques -- Code of Practice for Protection of Personal Information (PI) in Public Clouds Acting as PI Processors
- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)
  - Center for Internet Security (CIS)
  - Department of Defense Cybersecurity Agency (DISA) Secure Technology Implementation Guides (STIGs)
  - Generally Accepted Privacy Practices (GAPP)
  - Fair Information Practice Principles (FIPP)
  - Control Objectives for Information and Related Technologies (COBIT)
  - Privacy by Design (PbD)
  - AuditScripts. Open Threat Taxonomy
  - European Union Regulation 2016/279 (General Data Protection Regulation (EU GDPR))
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Gramm-Leach-Bliley Act (GLBA)
  - Family Educational Rights and Privacy (FERPA)
  - Protection Of Pupil Rights Amendment (PPRA)