Data Privacy and Security Policy

CNMI P20W Data Governance Committee

REFERENCES:

Originator	Data Privacy and Security Subcommittee
Effective Date	May 28, 2025
Approved by	CNMI P20W Executive Leadership
Statutory Reference	1. Family Educational Rights and Privacy Act (FERPA) of 1984 (20 U.S.C. Sec. 1232g; 34 CFR Part 99); 2. Internal Revenue Code of 1954 (26 CFR Part 601) 3. CNMI State Board of Education Regulations (Title 60-20) 4. CNMI Statistical Act of 1990 (CNMI P.L. 7-35) 5. Establishment of Northern Marianas Technical Institute (3 CMC §12104) 6. Establishment of Department of Commerce: 1 CMC §2451 7. Establishment of Department of Finance: 1 CMC §2551 8. Establishment of Department of Labor: 1 CMC §2831 9. Establishment of Department of PSS: 1 CMC §2251 10. Establishment of Department of NMC: 3 CMC §1304

PURPOSE

This Data Privacy and Security Policy establishes a comprehensive framework for managing and protecting data across the CNMI P20W longitudinal data system. It ensures the protection and appropriate use of data, with a particular focus on personally identifiable information (PII), business identifiable information (BII), and sensitive educational records. The primary goals of this policy are to ensure data confidentiality, integrity, and availability; safeguard PII and BII; establish standardized procedures for data management; support the mission of CNMI institutions while maintaining strict data protection standards; and comply with all applicable federal and CNMI data privacy and security regulations.

SCOPE

The policy applies to all appointed P20W Data Governance Committee (DGC) members (data stewards & IT reps), DGC proxies, CNMI P20W Executive Leadership, respective vendors and

all other parties involved in the privacy and security of data to the SLDS P20W data warehouse. It covers all forms of data privacy and security.

DEFINITIONS

1. Access Controls: Controls that limit entry to information system resources to authorized users, programs, processes, or other systems.
2. Availability: Ensuring that data, systems, and services are accessible and usable when needed by authorized individuals. This involves implementing measures to maintain high system uptime and prevent service disruptions.
3. Business Identifiable Information (BII)**:** Information that can be used to identify a business or organization, including but not limited to business tax ID numbers, business names, addresses, financial information, and trade secrets that could cause harm or competitive disadvantage if disclosed.
4. Confidential Data: Data classified as sensitive information that include information about the identity of individuals and employers.
5. Confidentiality: Protecting information from unauthorized access and disclosure.
6. Data Classification: The process of organizing data into categories that make it easier to retrieve, protect, and use. This involves identifying the types of data, assessing its sensitivity, and applying appropriate labels or categories to it.
7. Data Governance: Overall management of data availability, usability, integrity, and security.
8. Data Minimization: Limiting data collection to what is necessary for the intended purpose.
9. Data Security: Safeguards to protect PII from unauthorized access, use, disclosure, disruption, modification, or destruction.
10. Data Sharing: Practice of making data available to others for use, analysis, or collaboration.
11. Data Steward: Responsible for the management and oversight of data assets.
12. Educational Records: Information maintained by an educational agency or institution related to a student.
13. FERPA: The Family Educational Rights and Privacy Act, protecting student education record privacy.
14. Incident Management: Structured process for responding to unplanned events or incidents that disrupt normal operations or pose potential threats to an organization's infrastructure, services, or data. The primary goal is to restore normal operations as quickly as possible while minimizing impact and preventing future incidents.
15. Integrity: Guarding against improper information modification or destruction.
16. Internal Data: Data intended to be used by the SLDS and/or any of the CNMI P20W partner agencies and not meant for public disclosure.

17. Personally Identifiable Information (PII): Information that can be used to identify an individual.
18. Public Data: Data classified as information that is not sensitive and can be freely shared with the public.
19. Restricted Data: Data classified as highly sensitive (such as personally identifiable information) information that could cause significant harm or legal liability if disclosed.

RELATED DOCUMENTS:

1. *Memorandum of Understanding between CNMI Department of Commerce, CNMI Department of Finance, CNMI Department of Labor, Northern Marianas College, Northern Marianas Technical Institute and CNMI Public School System*
   - Attachment A: P20W Data Governance Program Charter, Section V - Policies and Processes, subsection *(m) Data Security*
2. *CNMI P20W Data Transfer Policy*

STATEMENT

The CNMI government agencies and educational institutions covered by this policy are committed to protecting the data privacy and security of all data under their stewardship.

1. Data Classification and Management
   - All data must be classified according to sensitivity levels (Restricted, Confidential, Internal, Public) with handling procedures aligned to classification
   - Data should only be collected for specified, explicit, and legitimate purposes, applying data minimization principles
   - Procedures must be implemented to ensure data accuracy, completeness, and currency throughout its lifecycle
   - Data must be retained only as long as necessary or required by law, with secure disposal methods used

2. Privacy and Access Controls
   - Informed consent must be obtained for personal data collection and use, with clear privacy notices provided
   - Only authorized personnel should have access to data, implementing appropriate authentication and access controls
   - Inter-agency data sharing must be governed by formal agreements, and disclosures to third parties must comply with legal regulations

3. Security and Integrity Protections
    - Appropriate technical and organizational measures must protect data from unauthorized access, transmission, alteration, or destruction
    - Data processing activities must follow documented procedures with clear audit trails maintained
    - Data must be stored using secure, approved systems with appropriate encryption and backup measures
    - Storage locations must comply with data residency requirements, with clear documentation of storage architecture

4. Incident Management and Response
    - Any data security incidents, such as breaches or unauthorized access, must be reported immediately to the Data Governance Manager (DGM) and SLDS Director
    - DGM will liaise with P20W Executive Leadership regarding incidents
    - An incident response plan will be created and updated by the DGC to address and mitigate potential risks
    - Until a formal plan is established, the National Institute for Standards and Technology (NIST) cybersecurity framework will be applied

RESPONSIBILITIES

1. CNMI P20W partner agency shall:
    a. Adhere to the data privacy and security policy
    b. Perform data classification prior to handling sensitive data
    c. Implement appropriate privacy and security controls
2. CNMI P20W Executive Leadership shall review and approve privacy and security measures within their respective agencies
3. CNMI SLDS program shall:
    a. Be responsible for ensuring the effective implementation of this policy
    b. Report all data privacy and security incidents to CNMI P20W Executive Leadership
4. Data Stewards shall serve as the primary point of contact for data privacy and security matters

COMPLIANCE

Adherence to this policy is mandatory. Compliance will be monitored through regular audits, continuous monitoring, self-assessments, and incident reporting. Enforcement actions for violations may include additional training.

TRAINING

- Outreach and awareness training will be conducted in phases at each partner agency by the CNMI P20W Data Governance Committee to keep informed about the importance of data protection
    - Phase 1 (Goals), Phase 2 (Process), Phase 3 (Content)
- Personnel directly involved in data privacy and security shall receive regular training on data protection procedures and security best practices

COMMUNICATION

- This policy shall be distributed to all CNMI P20W Data Governance Committee members and their agency personnel directly involved in the implementation of data privacy and security measures
- This policy will be stored electronically for access on a secured shared drive: P20W DGC Approved Policies

REVISION HISTORY

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	05/2025	Initial policy