Data Transfer Policy

CNMI P20W Data Governance Committee

REFERENCES:

Originator	CNMI P20W Data Governance Committee
Effective Date	October 15, 2024
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 USC 6103; 26 CFR) 3. CNMI Statistical Act of 1990 (CNMI P.L. 7-35) 4. The Education Act of 1998 (CNMI P.L. 6-10) 5. Postsecondary Education Act of 1984 (CNMI P.L. 4-34) 6. Establishment of Northern Marianas Trades Institute (CNMI P.L. 20-92) 7. CNMI Department of Finance (1CMC §2551, 1CMC § 2553, 1CMC §2557) 8. CNMI Department of Commerce (Executive Order 94-3 §103) 9. CNMI Department of Labor (Executive Order 94-3 § 301)

PURPOSE:

The purpose of this policy is to ensure that the transfer of data from each of the CNMI P20W partner agency source to the CNMI Statewide Longitudinal Data System (SLDS) P20W data warehouse is secure and efficient with the goal of protecting its integrity, confidentiality, and availability of information. Additionally, this policy establishes the expectations for regular data refresh intervals and the timely updating of each data source to maintain the accuracy and relevance of the information within the system.

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 transfer of data to the SLDS P20W data warehouse. It covers all forms of data transfer.

DEFINITIONS:

1. Access Controls: Controls that limit entry to information system resources to authorized users, programs, processes, or other systems.

2. Confidential Data: Data classified as sensitive information that include information about the identity of individuals and employers.
3. Data: Any information that is processed, stored or transmitted from a CNMI P20W partner agency source to the SLDS P20W data warehouse.
4. 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.
5. Data Transfer: The act of moving data from one location to another.
6. Encryption: The process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.
7. P20W data warehouse: The repository of data that links and stores data from all CNMI P20W partners.
8. 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.
9. 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.
10. Public Data: Data classified as information that is not sensitive and can be freely shared with the public.
11. 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 Institute and CNMI Public School System*
    a. Attachment A: P-20W Data Governance Program Charter, Section V - Policies and Processes, subsection ***(a) SLDS Expansion*** & *(m) Data Security*

STATEMENT:

1. Authorization and Approval
    - All data transfers must be authorized and approved by the respective CNMI P20W Executive Leadership member and SLDS Director.
2. Data Classification
    - Data must be classified according to its sensitivity and security. Classification levels include: Restricted, Confidential, Internal & Public.
    - Level of security measures for data transfer should correspond to its classification.

- A data classification policy shall be developed and maintained by the DGC.

3. Data Transfer Methods
    - Electronic Transfer: Secure methods such as encrypted email, secure file transfer protocols (SFTP), or virtual private networks (VPN) via application programming interface (API) or extract, transform and load (ETL) processes.
    - Data transfer must be direct from partner agency source to the P20W data warehouse.
4. Encryption
    - All restricted, confidential and internal data must be encrypted during transfer using industry-standard encryption protocols.
    - Encryption keys must be managed and stored securely.
5. Access Control
    - Only authorized personnel should have access to data being transferred.
    - Access controls, such as password and multi-factor authentication, must be implemented.
6. Monitoring and Logging
    - All data transfers will be monitored and logged by the SLDS Program and contributing partner agency to ensure compliance with this policy.
    - Logs must include details such as the date and time of transfer, data transferred, parties involved, and method used.
7. Incident Management
    - Any data transfer incidents, such as data breaches or unauthorized access, must be reported immediately to the Data Governance Manager (DGM) and SLDS Director. DGM will then liaise to the P20W Executive Leadership.
    - An incident response plan will be created (and updated) by the DGC to address and mitigate potential risks. Until such time, 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 transfer policy
    b. perform data classification prior to data transfer into the SLDS P20W data warehouse
    c. extract and validate data
2. CNMI P20W Executive Leadership shall review and approve data transfer from their respective agencies.
3. CNMI SLDS program shall:
    a. be responsible for ensuring the effective implementation of this policy
    b. report all data transfer incidents to CNMI P20W Executive Leadership

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 transfer.
    - Phase 1 (Goals), Phase 2 (Process), Phase 3 (Content)
- Personnel directly involved in data transfer shall receive regular training on data transfer 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 transfer from their source to the SLDS P20W data warehouse.
- 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	10/2024	Initial policy
2	03/2025	Remove legal action in compliance section