CNMI PSS | COMMONWEALTH OF THE NORTHERN MARIANA ISLANDS PUBLIC SCHOOL SYSTEM

Privacy Framework for CNMI Public School System (PSS)

Purpose and Objectives

This Privacy Framework is designed to protect the privacy of students, faculty, staff, and stakeholders by aligning with the National Institute of Standards and Technology (NIST) Privacy Framework. It establishes guidelines to manage privacy risks, safeguard sensitive information, and ensure compliance with local, federal, and international privacy regulations, including FERPA.

Key Objectives:

1. Protect personal and sensitive information of students, staff, and stakeholders.
2. Promote a culture of privacy awareness and accountability across all departments.
3. Align privacy practices with legal and regulatory requirements.
4. Enhance transparency and trust with all stakeholders regarding data practices.
5. Enable the secure and ethical use of data to improve educational outcomes.

Framework Core Functions

The framework adopts the NIST Privacy Framework's core functions: **Identify, Govern, Control, Communicate, and Protect.**

1. Identify

- **Inventory and Mapping**:
    - Maintain an up-to-date inventory of data repositories containing sensitive information, such as student records, staff files, and assessment data.
    - Identify data flows within and outside the district (e.g., third-party vendors, cloud services).
- **Privacy Risk Assessment**:
    - Conduct regular privacy risk assessments to evaluate how data is collected, processed, and shared.

    - Assess privacy risks associated with new technologies or software adopted by the district.
- **Data Classification**:
    - Classify data by sensitivity level (e.g., public, internal, restricted) to prioritize privacy measures.

2. Govern

- **Privacy Governance Policies**:
    - Establish a privacy governance committee to oversee data privacy initiatives and address privacy concerns.
    - Develop policies to define roles and responsibilities related to privacy management.
- **Compliance Management**:
    - Ensure adherence to privacy regulations, such as FERPA, CIPA, and GDPR (if applicable).
    - Regularly audit privacy practices for compliance.
- **Vendor Privacy Management**:
    - Require data protection agreements with third-party vendors and service providers.
    - Ensure vendors meet privacy standards for handling district data.

3. Control

- **Access Management**:
    - Implement role-based access control (RBAC) to restrict access to sensitive data based on job responsibilities.
    - Use multi-factor authentication (MFA) for accessing sensitive systems.
- **Data Minimization**:
    - Collect only the minimum amount of data necessary for educational and administrative purposes.
    - Regularly review and delete unnecessary data.
- **Data Retention and Disposal**:
    - Establish retention schedules for sensitive data and ensure secure disposal of outdated records.

4. Communicate

- **Transparency and Notice**:
    - Publish privacy notices to inform stakeholders about data collection and use practices.
    - Ensure clear communication with parents, students, and staff about privacy rights.
- **Privacy Awareness Training**:

    - Provide mandatory privacy training for staff and content managers handling sensitive data.
    - Include privacy education in student digital literacy programs.
- **Incident Notification**:
    - Develop procedures for timely notification of data breaches or privacy incidents to affected parties and regulatory authorities.

5. Protect

- **Data Security Measures**:
    - Encrypt sensitive data at rest and in transit.
    - Use secure data transfer protocols when sharing information with third parties.
- **Monitoring and Auditing**:
    - Monitor data access and usage logs for unauthorized activities.
    - Conduct regular audits to ensure compliance with privacy policies.
- **Incident Response**:
    - Integrate privacy considerations into the district's cybersecurity incident response plan.
    - Investigate privacy incidents to identify root causes and prevent recurrence.

Implementation Strategy

To operationalize this framework, PSS will:

1. Establish a cross-departmental Privacy Committee to oversee implementation.
2. Conduct a district-wide data inventory and risk assessment.
3. Develop privacy-focused training programs for staff and students.
4. Collaborate with IT to integrate privacy controls into technology systems.
5. Regularly review and update policies to address emerging privacy risks.

Conclusion

The CNMI Public School System is committed to safeguarding privacy by aligning with the NIST Privacy Framework. Through this Privacy Framework, PSS will build a robust privacy culture that protects personal information, enhances trust, and ensures compliance with regulatory requirements.