CNMI Public School System

Data Privacy & Security Manual

Version 1.0
May 2025

COMMONWEALTH OF THE
NORTHERN MARIANA ISLANDS
PUBLIC SCHOOL SYSTEM

Table of Contents

1.1 Introduction

The CNMI Public School System (PSS) is committed to protecting the privacy and security of student and staff data in compliance with federal and local laws, regulations, and best practices. As reliance on technology and data systems grows, safeguarding personally identifiable information (PII) is essential to maintaining public trust and ensuring the integrity of educational operations. This Data Security and Privacy Manual offers a structured and comprehensive approach to implementing a data security program that aligns with national standards—such as FERPA and the NIST Privacy Framework—as well as the CNMI PSS Data Governance Manual. Developed through the collaborative efforts of PSS, including the Statewide Longitudinal Data System (SLDS), the Office of the State Infrastructure Technology (SIT), and the Data Governance Committee (DGC), the manual reflects a unified commitment to creating a secure and resilient data environment.

1.2 Purpose and Scope

The purpose of this plan is to assist the PSS, including central office departments and school sites, in developing and maintaining a robust and responsive data security and privacy program. This program supports the broader goals of the PSS Data Governance Committee and is vital to preserving confidentiality, integrity, and availability of sensitive education data.

This plan applies to all PSS staff, contractors, vendors, and stakeholders who handle, manage, or access PSS information systems or data. It includes both physical and electronic security components and encompasses all assets that process, store, or transmit educational records and other sensitive information.

The successful implementation of data privacy and security at PSS required active participation form key governance bodies and assigned personnel. The roles below define the responsibilities of each entity in safeguarding student and staff data and ensuring regulatory compliance

2.1 Statewide Longitudinal Data System Program (SLDS)

The SLDS Program leads data system design and integration with a heavy focus on privacy and security. It:

- Provides technical leadership in designing and implementing secure data systems.
- Facilitates the integration of privacy and security measures into data collection and reporting tools.
- Supports training initiatives related to secure data handling and reporting.

2.2 Data Governance Committee (DGC)

The DGC oversees the development, implementation, and revision of data governance and privacy and security policies. It:

- Reviews security risks and ensure alignment of practices with the PSS strategic objectives.
- Promotes cross-departmental collaboration to address data security issues.
- Advises on the approval and periodic review of technology tools and vendors for compliance with FERPA, PPRA, and PSS privacy standards.

2.3 State Infrastructure Technology (SIT) Office

The SIT Office enforces the technical safeguards that protect PSS data. It:

- Implement and maintain technical safeguards such as firewalls, antivirus software, secure configurations, multi-factor authentication, and encryption to protect PSS data systems.
- Conduct regular system and network monitoring to detect, assess, and respond to security vulnerabilities, unauthorized access, or anomalous activity.
- Perform vulnerability assessments and apply timely patches and updates to mitigate known risks and strengthen infrastructure resilience.
- Coordinate with the Data Privacy Specialist and PSS Leadership to execute data breach response protocols, including incident containment, documentation, investigation, and recovery.
- Ensure secure access management, including role-based access controls, authentication protocols, password policies, and audit trails for all PSS systems and devices.
- Maintain a comprehensive inventory of all devices, servers, applications, and third-party systems that store or transmit PSS data.
- Manage secure data backup and disaster recovery procedures to ensure continuity of operations and availability of critical education data.
- Support the vetting and integration of third-party software and platforms, ensuring compliance with district data privacy and security requirements.
- Collaborate with other departments and schools to ensure proper implementation of technical security measures across all campuses and administrative sites.

2.4 Data Privacy Specialist

The Data Privacy Specialist works closely with the SLDS Project Director and DGC to establish and enforce organizational privacy policies that govern PSS' data collection, sharing, and use including but not limited to:

- User access policies that limit access to only those with a legitimate need,
- Data retention and destruction schedules that are based on the uses of the data,
- Data minimization guidelines that ensure that the organization collects the minimum amount of data necessary to fulfill stated need(s), and
- Statistical methods for disclosure avoidance of identifiable information regarding any publicly reported data
- Provide training on privacy best practices and legal compliance

- Develop and oversee implementation of data incident response.
- Create and implement a cybersecurity plan that is in line with industry standard best practices.

Support procurement of technology and data tools and systems by:

- Providing guidance during the evaluation process to ensure that products that meet the standards of the PSS' privacy and security policies,
- Training third parties on PSS' privacy and security policies and standards, and
- Ensuring contracts and data sharing agreements include appropriate privacy and security protections
- Review and approve data that have been requested by external parties as well as data systems that will include sensitive information prior to release to ensure they comply with the organization's policies.

Coordinate privacy and security audits:

- Provide guidance to the executive team and staff on how to achieve their goals while protecting privacy as well as develop privacy advocates throughout PSS to ensure effective implementation of privacy protections.
- Conduct an annual data security training for all data governance members and stakeholders with access to PII

Personnel Security is vital to protecting the confidentiality, integrity, and availability of PSS data systems. All employees, contractors, school officials, and third-party partners share the responsibility of safeguarding educational records and digital assets. This guideline outlines expectations for acceptable technology use, legal compliance, data handling, and training to ensure responsible behavior and regulatory alignment.

3.1 Acceptable Use Policy & Legal Compliance

The PSS maintains an Acceptable Use Policy (AUP) that outlines the appropriate and inappropriate uses of its Internet, Intranet, and Extranet systems. The AUP is designed to ensure safe, responsible, and ethical use of technology by all users within the school system.
The AUP applies to:

- **Students**, through the Acceptable Use Agreement (AUA)
- **Employees and contractors,** via on-boarding compliance and technology use guidelines
- **Third-party vendors**, as outlined in contracts or service agreements

Policy Update Status

These Technology Regulations are currently under review and pending final approval, which will be made available on the official legal resource site: § 60-20-540 Library, Media, and Technology Services; Student Internet Usage and § 60-30.2-370 Internet Usage and Local laws, such as PSS Rules and Regulations § 60-30.3-268 Internet Usage

The updated AUP will:

- Provide clearer guidance on acceptable and prohibited activities
- Reflect advancements in technology and cybersecurity standards
- Align with federal and local legal requirements and best practices
- Be integrated into onboarding and annual compliance training for all relevant users.

3.2 Employee Rules and Procedures

These rules ensure that every employee and affiliate engaging with PSS data systems upholds privacy, security, and legal integrity.

3.2.1 Confidentiality Agreements and Training Requirements

- All personnel must sign a confidentiality agreement prior to data access.
- Completion of required training is mandatory before accessing data systems:
  - FERPA 101: For Local Education Agencies
  - FERPA 201: Data Sharing under FERPA
  - PSS Privacy and Security Awareness Training: With annual recertification
- Contractors and vendors must complete all mandated certifications and clearances prior to being granted access.

3.2.2 Legal and Policy Compliance

All personnel must comply with:

- Federal laws, such as FERPA (20 U.S.C. § 1232g; 34 CFR Part 99)
- Local laws, such as PSS Rules and Regulations § 60-20-428
- Local laws, such as PSS Rules and Regulations § 60-30.3-268
- Internal policy requirements, contractual obligations, and licensing terms
- Background checks are required for all employment offers

3.2.3 Data Handling and Software Use Best Practices

Employees must adhere to secure practices that minimize the risk of data breaches:

- Remain alert to security and privacy threats
- Protect login credentials and access tokens:
  - Never share passwords or write them in visible locations
  - Report suspected compromise immediately to a supervisor
- Refrain from actions that compromise the security or integrity of any PSS system

By following this unified Personnel Security guideline, PSS personnel contribute to a trustworthy and secure educational environment. Regular compliance and vigilance are essential to protecting sensitive data and upholding the mission of the CNMI Public School System.
To safeguard the confidentiality, integrity, and availability of PSS data, access is strictly controlled through a combination of user authentication mechanisms and access management protocols. This manual establishes the minimum requirements for authenticating access to information systems within the PSS network, including systems managed by third-party vendors and contractors.

4.1 Authentication Requirements

Access to PSS data systems shall be restricted to authorized personnel based on role, responsibility, and need-to-know. All users, including employees, contractors, and third-party vendors, must authenticate using secure methods aligned with industry best practices and the PSS cybersecurity framework.

4.1.1 Two-Factor Authentication (Multi-Factor Authentication - MFA)

To enhance security, domain access must be coupled with a second factor of authentication, such as:

- Mobile authenticator app (push notification approval).
- Voice-based confirmation via office or personal phone.
- One-time passcodes delivered via SMS or email.
- Two-factor authentication is recommended for all access to systems housing sensitive or personally identifiable information (PII). PSS reserves the right to implement additional password complexity requirements, expiration periods, and monitoring tools to ensure compliance with cybersecurity standards.

The Public School System (PSS) acknowledges the critical importance of safeguarding sensitive information, particularly when transmitted via email. The transmission of unprotected Personally Identifiable Information (PII) or other forms of sensitive data presents a substantial security risk. Unauthorized access or disclosure of such information can result in severe consequences, including identity theft, financial fraud, reputational harm, and potential legal liabilities. To address these risks, it is imperative that organizations implement secure methods for data transmission. Recommended technical solutions include the use of encrypted file transfers, secure file-sharing platforms, and encrypted email services to ensure the protection of data both in transit and at rest.

These practices include:

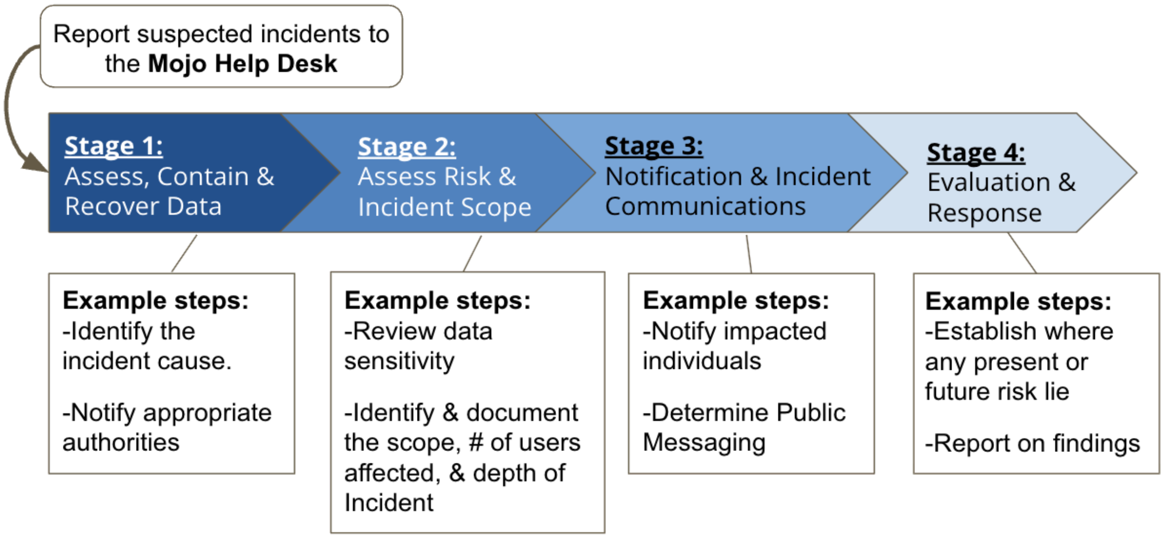
- Data Minimization and Masking: Redacting, anonymizing, or desensitizing data before transmission to limit exposure of sensitive information.

- Restricting Email Recipients and Content: Verifying recipient email addresses before sending sensitive data and limiting the use of email for highly confidential communications.
- It is recommended that all student data transmitted via email be encrypted and password-protected.

CONFIDENTIALITY NOTICE:
This message (including any attachments) may contain confidential, proprietary, privileged and/or private information. The information is intended to be for the use of the individual or entity designated above. If you are not the intended recipient of this message, please notify the sender immediately, and delete the message and any attachments. Any disclosure, reproduction, distribution or other use of this message or any attachments by an individual or entity other than the intended recipient is prohibited.

By following these best practices, PSS enhances its commitment to protecting sensitive information and ensuring compliance with data security regulations.
When an incident does occur it is critical to have a process in place to both contain and fix the problem. Procedures for users, security personnel, and managers need to be established to define the appropriate roles and actions. Outside experts may be required to do a forensics investigation of the incident, but having the correct procedures in place initially will minimize the impact and damage. PSS has a SOP in place to activate when an incident happens Incident Response Plan (IRP) for users, security personnel, and managers to take action on this matter.

Incidents Response Plan (Flowchart)



Report suspected incidents to the **Mojo Help Desk**

Stage 1: Assess, Contain & Recover Data

Stage 2: Assess Risk & Incident Scope

Stage 3: Notification & Incident Communications

Stage 4: Evaluation & Response

Example steps:
-Identify the incident cause.

-Notify appropriate authorities

Example steps:
-Review data sensitivity

-Identify & document the scope, # of users affected, & depth of Incident

Example steps:
-Notify impacted individuals

-Determine Public Messaging

Example steps:
-Establish where any present or future risk lie

-Report on findings

The SIT Office is responsible for overseeing the security and integrity of the PSS network, including all endpoint devices such as desktops, laptops, mobile devices, and servers. All PSS

System Administrators are required to ensure that the systems they manage comply with the security standards based on the guidance of the NIST Privacy Framework. These controls are designed to provide a defense-in-depth cybersecurity approach that mitigates risk and protects PSS's sensitive educational data and digital infrastructure.

Each domain below describes a critical security practice that is implemented across PSS systems.

7.1 Inventory and Control of Hardware Assets

- Maintain an active inventory of all managed hardware devices on the network.
- Ensure only authorized devices are granted access.
- Identify and prevent access by unauthorized or unmanaged devices.

7.2 Inventory and Control of Software Assets

- Maintain an accurate inventory of all software installed on PSS managed devices.
- Ensure only authorized software is permitted to run.
- Prevent installation or execution of unauthorized or unmanaged software.

7.3 Continuous Vulnerability Management

- Continuously monitor for new vulnerabilities.
- Implement timely patching and remediation to reduce attack exposure.
- Use vulnerability assessment tools to inform risk mitigation strategies.

7.4 Controlled Use of Administrative Privileges

- Implement strict controls over the assignment and use of admin-level privileges.
- Regularly audit, track, and revoke unnecessary privileges.
- Prevent misconfigurations and privilege misuse.

7.5 Secure Configuration for Hardware and Software

- Apply standardized secure configurations to all managed endpoints (mobile devices, laptops, workstations, servers).
- Use configuration management and change control processes to enforce and monitor compliance.

7.6 Maintenance, Monitoring, and Analysis of Audit Logs

- Enable logging on all critical systems.
- Collect, manage, and analyze logs for suspicious activities and potential breaches.
- Retain logs for a minimum of 30 days to support investigations.

7.7 Endpoint Protections

- Harden email and browser configurations to reduce phishing and social engineering risks.
- Use enterprise-grade malware protection tools across all network and endpoint layers.
- Enable automated updates and real-time scanning for malware detection.

- Monitor endpoint and malware-related activity and take immediate corrective action when needed.

7.8 Limitation and Control of Network Ports, Protocols, and Services

- Restrict open ports and unused services to the minimum necessary.
- Monitor and control changes in network communication pathways.

7.9 Data Recovery Capabilities

- Implement regular, secure backups of critical data.
- Test recovery procedures routinely to ensure data can be restored quickly and accurately.

7.10 Boundary Defense

- Establish defenses between trusted and untrusted networks.
- Use firewalls, intrusion detection/prevention systems (IDPS), and data loss prevention (DLP) tools to enforce boundary protection.

7.11 Data Protection

- Implement safeguards to prevent unauthorized data access and exfiltration.
- Use encryption, access controls, and data classification frameworks to protect sensitive information.

7.12 Controlled Access

- Grant access to resources and information only to individuals and systems with a verified need and authorization.
- Regularly review and audit access rights based on roles and responsibilities.

7.13 Wireless Access Control

- Secure all wireless infrastructure including WLANs, access points, and wireless clients.
- Use strong encryption, access authentication, and monitoring for rogue devices.

The PSS Security Standards represent a foundational component of the school system's cybersecurity framework. Adherence to these standards is mandatory for all stakeholders utilizing or managing PSS technology resources. Compliance supports the confidentiality, integrity, and availability of educational data and helps maintain a secure digital environment for students, staff, and partners.

“The Data Security and Privacy Manual was reviewed and approved by a member of the PSS DGC, SLDS Project Director, SIT Office, and Data Privacy Specialist. These entities are responsible for establishing best practices in audit, monitoring, and incident response as described in this manual.”

Final Approver:

Jesse Tenorio
State Infrastructure Technology Director
CNMI Public School System

Date	Notes/Updates	Reviewer	Version
May 2025	Initial Release of the Data Security & Privacy Manual	DGC. SLDS Project Director, SIT Director	1.0