User Access Levels for Data Systems Policy

CNMI PSS Data Governance Committee

REFERENCES:

Originator	*Data Governance Committee*
Effective Date	*June 11, 2025*
Approved by	*CNMI PSS Executive Leadership*
Statutory Reference	The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. Sec. 1232g; 34 CFR Part 99) Health Insurance Portability and Accountability Act (HIPAA)

PURPOSE:

This policy aims to maintain the best practices of data privacy and security by managing user access levels across all district data systems and ensuring access to sensitive information is appropriately controlled and protected. It is essential to safeguard highly confidential data, ensure compliance with legal and regulatory requirements, and protect the integrity of all district information systems from misuse, breaches, and unauthorized access.

SCOPE:

This policy applies to all PSS stakeholders, including employees, contractors, vendors, and School Officials with access to data systems. The scope covers all data systems used within the CNMI Public School System.

POLICY STATEMENT:

This policy establishes guidelines for allocating, administrating, and withdrawing user access to data systems, safeguarding data confidentiality and security, and adhering to all relevant federal, local, and district policies and regulations.

1. User access to CNMI PSS data systems will be granted based on specific roles and responsibilities to ensure users only access data relevant to their job functions.

2. All user access levels will be reviewed and validated annually to maintain appropriate and secure access. User activities will be monitored and logged to detect unauthorized access or misuse.

3. Users will only be granted the minimum level of access necessary to perform their duties. Elevated or administrative access will require formal approval and be subject to regular audits to minimize security risks.

4. Access rights will be immediately revoked upon an employee's departure, role change, or contract completion to prevent unauthorized access.

5. When available, all users with access to highly confidential data must enable multi-factor authentication (MFA) for added security. Users must keep their credentials confidential and follow all authentication security measures, including password complexity rules and regular updates.

6. Temporary access will be granted only when necessary, with predefined expiration dates and strict monitoring. Contractors, vendors, and third-party service providers will receive limited and controlled access based on contractual requirements, with periodic access reviews to ensure compliance.

7. Users must agree to and comply with data sensitivity classifications, ensuring they handle, store, and share data according to legal and organizational policies.

8. All user access requests or modifications must be submitted for approval to the District Manager/Administrator, or their designee, prior to accessing any system.

9. All access requests must follow a documented approval process, including verification of need and supervisor authorization. Guest access will be managed separately through an Access Request Form.

RESPONSIBILITIES:

The access level of a user and the duration for which access is granted will be determined by the District Manager/Administrator of the specific platform or program, or their designated representative. To protect sensitive information and ensure secure access across all district systems, the following requirements and oversight responsibilities are established:

1. The District Manager/Administrator must:
    - Ensure proper oversight and security of user access.
    - Conduct a review of user access levels annually or when significant role changes occur.
    - Modify or terminate access upon changes in duties or separation from employment.

2. The Data Governance Committee (DGC) and SLDS Data Privacy Specialist will:
    - Review and validate all user access levels on an annual basis.
    - Monitor and log user activity to detect unauthorized access or misuse.

3. District Manager/ Administrator:
    - Rights: Full rights to all system functions, including user management, system configuration, and data access,
    - Responsibilities: Managing system settings, creating and deleting user accounts, and overseeing overall system security.

4. Department Head/Manager:
    - Rights: Rights to data and reports relevant to their department, ability to approve access requests, and manage team permissions
    - Responsibilities: Ensuring team members have appropriate access, reviewing access levels regularly, and reporting any security issues.

5. Employee:
    - Rights: Rights to data and applications necessary for their specific job functions.
    - Responsibilities: Using data responsibly, adhering to security policies, and reporting any unauthorized access.

6. Contractor, Vendors, and third-party service providers:
    - Rights: Limited rights to specific data and systems required for their contracted tasks.
    - Responsibilities: Complying with all security policies and only accessing data necessary for their work.

7. Guest:
    - Rights: Very limited rights, typically read-only, to specific data or systems for a short duration.
    - Responsibilities: Following all security guidelines and only accessing data as permitted.

RELATED DOCUMENTS:

1. **PSS Acceptable Use Agreement**
2. **PSS Data Governance Executive Policy**: Outlines the overall data governance framework within PSS, including data management, access controls, and data security protocols.

DEFINITIONS:

1. **Access:** means the ability for an authorized user to view or manipulate data in the systems maintained by PSS.

2. **Access Levels:** Categories of permissions assigned to users that determine their ability to interact with data systems (e.g., Administrator, User, Read-Only).
3. **Read-Only Access**: Users can view data but cannot make changes.
4. **Write Access**: Users can modify existing data and add new data but cannot delete data.
5. **Administrative Access**: Users have full control over data and system settings, including adding or removing other users, modifying access levels, and modifying, adding, and deleting data.
6. **Custom Access**: Specialized access tailored to specific roles or needs, and are subject to additional approval.
7. **Confidentiality:** any record or information not open for public inspection or where disclosure is restricted pursuant to relevant federal or state statutes or regulations.
8. **Data Systems**: Any digital platforms, databases, applications, or repositories that store, manage, or process organizational data.
9. **Unauthorized Access**: Access to data systems or data by individuals who do not have explicit permission to do so.
10. **User Credentials**: Information, such as usernames and passwords, that authenticate a user's identity and grant access to data systems.

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:
All employees, contractors, and third-party service providers will undergo mandatory training on user access levels for data systems. Refresher training will be conducted annually to reinforce and update knowledge.

COMMUNICATION:
This policy shall be distributed to all CNMI P12 Data Governance Committee members and personnel directly involved in the implementation. This policy will be stored electronically for access on the CNMI PSS or SLDS website and secured shared drive: P12 DGC Approved Policies.

REVISION HISTORY:

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	5/13/2025	Initial Policy