
# CNMI SLDS

## CHALLENGE

"We have not documented the user access levels for each data system in PSS. CDI #8)"

- PSS needs to document and update user access levels

## SOLUTION

Conduct inventory of data systems in PSS and document it here: https://bit.ly/46jFZtE

Document user access levels and associated permissions for each level of access

## OUTCOME

Schools and Central Offices will have internal procedural controls established to manage user data access, including security screenings, training, and confidentiality agreements required for staff with PII access privileges

Compliance with SIT, Federal & Local State Laws regarding data security and privacy such as FERPA

## CALL TO ACTION:

Conduct inventory of data systems in PSS and document it here: https://bit.ly/46jFZtE

| Office / Department / Program/School Users | Programs/Softwares | Technical Administrator(s) | UAL Documentation - Exists? | If yes, where is it available? | User Groups/Roles | Data Backup and Access? |
|---|---|---|---|---|---|---|
| Office Accountability, Research & Evaluation (Records & Data Management), All Schools (Role Based) | CNMI PSS Infinite Campus (Student Information System) | Ruth Calvo | Yes | For print; found within the program | Parents<br>Students<br>Teachers<br>Principals/Vice Principals<br>Registrars/Records Custodians<br>Attendance Officers<br>Counselors<br><br>Scheduler<br>Walk-in Scheduler | Backup - Infinite Campus Only<br>Sandbox Site - Exact copy of settings and data of the Live Site as of date of last refresh (until end of contract)<br>Staging Site - Exact copy of settings and data of the Live Site as of date of last refresh, DB Driven (until end of contract) |

COMMONWEALTH of the NORTHERN MARIANA ISLANDS
PUBLIC SCHOOL SYSTEM
PO BOX 501370, SAIPAN, MP. 96950 • TEL (670) 237-3061 • FAX (670) 664-3845
www.cnmipss.org
www.facebook.com/cnmipss | www.instagram.com/cnmipss | www.twitter.com/cnmi_pss



Donna M. Flores, M.S.
INTERIM COMMISSIONER OF EDUCATION
pss.coe@cnmipss.org

MEMORANDUM

DATE : September 22, 2023

TO : School Administrators, Program Leaders, and Department Senior Directors

FROM : CNMI PSS Data Governance Committee (DGC)

SUBJECT : User Access Levels Documentation Request and Survey

Greetings to all Leaders!

Your kind assistance is requested to confirm that your department has User Access Level (UAL) Documentation for the Data Programs that you administer for PSS. The Data Governance Committee is conducting an inventory on the UAL documentation for each of the PSS data programs. This is in conjunction with our committee's Critical Data Issue #8: ***We have not documented the user access levels for each data system in PSS.*** This was a concern posed by the US Department of Education through the Student Privacy Policy Office's Privacy Technical Assistance Center (PTAC). Acting on this CDI will strengthen the digital security processes of PSS. This will also mark the CNMI Public School System's transition from maintaining compliance-based strategies to being more proactive in utilizing mitigation risk strategies.

User Access Level is the permissions that are allowed or assigned to the different types of users. We have a sample UAL documentation provided by a data program attached for reference. This request should be provided to the administrator(s) of the program(s) utilized by your department. Also, as part of this task, we will need information of what programs your department or schools oversee. Input your information on the form provided at this link:

User Access Level-UAL-Documentation Form (https://bit.ly/46jFZtE)

You are not required to provide your programs' UAL documentation to the DGC, however, we highly recommend that this information be available and maintained at your department. We have provided 2 exhibits as references.

Exhibit 1: “IC functional user group descriptions-version5”
https://drive.google.com/file/d/1ycEM-EoxEzXDbt-uX8OdNXq392yz2F6n/view?usp=drive_link

Exhibit 2: “Renaissance User Permissions Table”
https://drive.google.com/file/d/1ATN49rd8NOy_shKLLM1d30IVrRKOc7Ri/view?usp=drive_link

Should you need more information please contact the Data Governance Committee at datagovernance@cnmipss.org.

Thank you,

Data Governance Committee - CDI#8
Email: datagovernance@cnmipss.org

# Significance of Recording User Access Levels

*Data Security & Privacy Question ---- Have internal procedural controls been established to manage user data access, including security screenings, training, and confidentiality agreements required for staff with PII access privileges?*

*Critical Data Issue: #8 We do have not documented the user access levels for each data system in PSS.*

*Proposed solution:*

- *Conduct inventory of data systems in PSS and document it here:* https://bit.ly/46jFZtE
- *Document user access levels and associated permissions for each level of access*

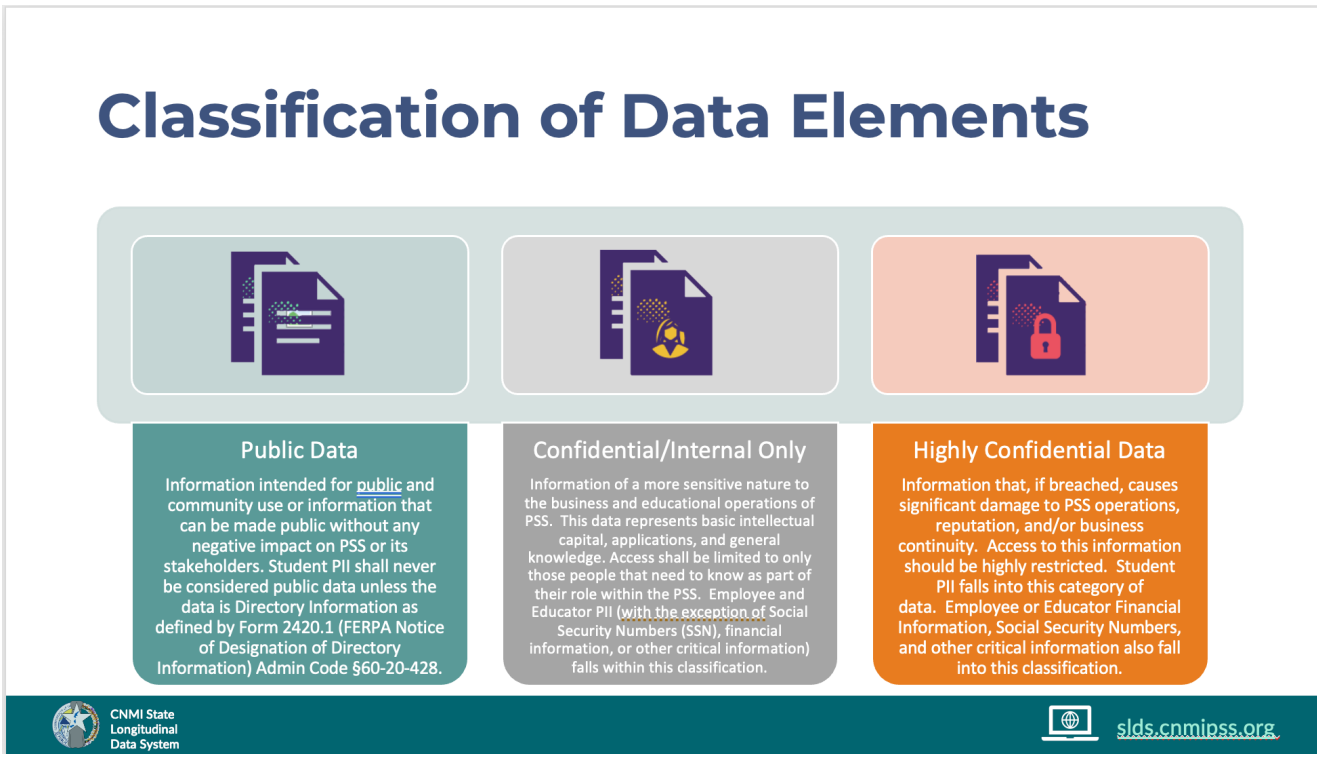
Why is documenting user access levels for each data system important?

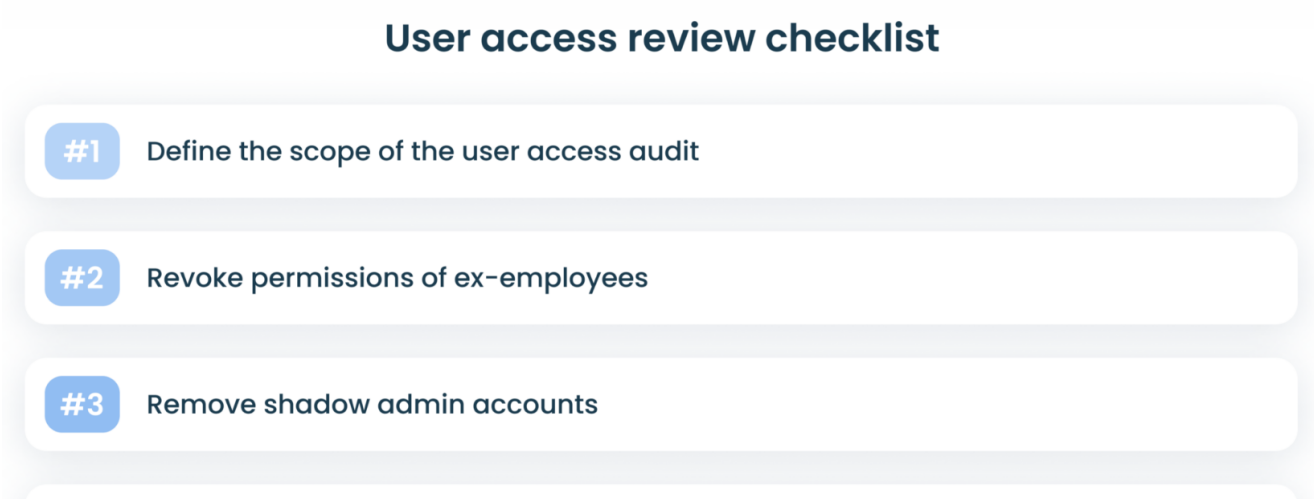
- Data Security - Confidentiality, Integrity, and Accountability
  - Create User Access Review Policy, Regulation, and SOP
    - Mitigate Data Security Issues (Origin: https://www.ekransystem.com/en/blog/user-access-review © Ekran System)
      - **Privilege creep** occurs when employees obtain access to more sensitive data than required while working at an organization. New privileges appear as employees gain new responsibilities and access rights without revoking the old ones.
      - **Privilege misuse** is when an insider uses granted privileges in a way that is different from or opposite to the intended use. Such actions may be unintentional, deliberate, or caused by ignorance. But no matter their cause, they often lead to cybersecurity threats.

- **Privilege abuse** is a fraudulent activity that involves an account with elevated privileges. Malicious actors may abuse privileges they were granted to access, exfiltrate, compromise, or damage an organization's confidential assets. Malicious insiders can abuse their privilege. As well, outside attackers can compromise privileged accounts and use their privileges for malicious purposes.
- During an access review, a security officer synchronizes users' access rights with users' current roles and limits employees' privileges to keep the risks of privilege creep, misuse, and abuse at a minimum.

- Compliance with SIT requirements, Federal & Local State Laws regarding data security and privacy such as FERPA

Resources:



#4 Ensure employees don't have access permissions from previous positions

#5 Make sure that employees and vendors have the fewest privileges possible

#6 Verify that permanent access is only given when necessary

#7 Analyze the results of the review and draw conclusions



## 6 best practices for user access audits