# MiSiS Staff Access Management
## *(Instructions for School Administrators)*

Managing your staff's access to the information contained in MiSiS is a critical responsibility for school administrators. The following document details some of the processes and tools available to administrators to assist them in managing access.

## *Contents*

## *Apply for Access to MiSiS*

### oneAccess Access Request System

Every employee authorized to view or modify student records, such as attendance or grades, must submit an authorization request through the oneAccessAccess Request System (https://oneaccess.lausd.net). Information on this system can be found on the MiSiS website (http://misis.lausd.net/) under **Apply for Access > oneAccess Access Request System**. Please note that Central Office staff, and Local District staff must use the manual paper application process described in the next section.

Step-by-step instructions for teachers and office staff can be found in the Guide to MiSiS User Roles.

### Paper Applications for Access

Central Office staff, and Local District staff must still use the manual process. The appropriate forms can be obtained by either clicking one of the forms below, or by going to the MiSiS website and clicking **Apply for Access** at the bottom of the page.

Access for District Offices Staff (Central Office and Region staff)

Production Mirror Access for School-Based Personnel (Central Office and Region staff that need school access)

- The appropriate MiSiS Access Request form must be submitted. **Please note: Submitting any version of the form that differs from that which is posted on the MiSiS website will result in immediate rejection of the application.**

- All information, unless marked "optional," is required for the processing of requests. Forms without a valid 8-digit employee number, user role, or signature, will be rejected. Access cannot be granted until the staff member's human resources (HR) record is completely processed, and all pending HR issues are resolved.

- Once the account is set up, the user and the administrator that provided the authorizing signature will receive confirmation via email.

New Employees

New employees, including teachers, cannot apply for access until the staff member's human resources (HR) record is completely processed and all pending HR issues are resolved. Once their SSO account is active, the user can use the oneAccess system to request access to MiSiS. Instructions for managing an SSO account can be found on the LAUSD – Single Sign On Console page.

Transferred Employees

Employees transferring from one school to another must submit a **new** oneAccess Request to gain access to the new school of assignment. Users are not automatically granted access to student records in their new location of employment. Please use oneAccess to "Remove Access from Previous School" if applicable.

## *Approving Access to MiSiS*

Instructions for administrators to approve staff access in OneAccess can be found in the OneAccess Approver User Guide.

***Note to Administrators: Before granting employee access requests, please review the Guide to MiSiS User Roles found on the MiSiS website under MiSiS > Training > Apply For Access. When approving user roles, administrators must consider the level of responsibility involved in the job assignment.***

## *Removing/Changing Staff Access to MiSiS*

To maintain confidentiality of information at the school, administrators should remove access for personnel (including previous administrators) who retire, move to another school, leave the District, or change job assignments at the same school. Removal of access is not automatic in any situation. **Administrators are responsible for making the appropriate access changes for current and former employees to prevent unauthorized access to confidential student and staff data.**

### Removal with oneAccess

Administrators can use oneAccess to manage the access (including removing access user roles) for staff that applied for access using the oneAccess system. Instructions for administrators to remove staff access can be found in the OneAccess Approver User Guide.

### Manual Removal of Access

To request removal of access for school staff who were approved manually, please submit the MiSiS Access Request Form for Region & Central Office Staff or Production Mirror Access for School-Based Personnel located on the MiSiS Website under MiSiS > Apply for Access and place an **R** by the roles to remove. Forms can be completed in writing or electronically, before being faxed. Please allow 1-2 business days for processing requests. Principals will receive an e-mail confirming receipt and processing of request. Please note that this form removes ALL access from MiSiS.

## *Security Audit Report*

In order to manage the security of MiSiS, this report provides information on who has access to your school's data. Schools should run this report every 6 months to ensure that your data is protected. The Security Audit Report offers a number of benefits, including:

1. The ability to manage access to the school's student information.
2. The information needed to remove or change access for employees that have left the school, or no longer need to view confidential student records.
3. The opportunity to decide which staff members should apply for access.

The report provides the information in multiple formats, such as PDF, Excel and Word. The report can be accessed via the following path after logging into MiSiS: Reports > Security > Security Audit Report.

How to read the report:
Last Name, First Name, Staff Number, and User Role Name are self-explanatory.

Status can be Active or Inactive

- Active –account with a future expiration date; user has access to your school data.
- Inactive –account with a past expiration date user could gain access to your school data if the account is reactivated when the user applies for access to another school. It is recommended to remove the user role assigned to your school.

Last Login – this is the last time the user successfully logged in with that user role; this is accurate as of the report's run time.

Staff Type – position information for Certificated personnel as provided by Human Resources. If the employee is Certificated and the field is blank, MiSiS has not received the information from Human Resources. If the employee is Certificated and holds more than one position at the school, the report will only display one position.

Data elements of the Security Audit Report:

- Location Code
- Employee Number
- School Name   User Role (s)
- Last Name
- Last Login Date
- First Name
- Staff Type

The following user roles can access this report:

- Office Manager
- Principal
- Scheduling Administrator

## *Forms and Documents for Managing Staff Access to MiSiS*

The documents below are relevant for manual management of staff access, and can be found on the MiSiS website at http://misis.lausd.net by clicking MiSiS > Apply for Access.

- To learn more about MiSiS user roles, refer to the Guide to MiSiS User Roles.

- To add or change user roles for schools and offices whose staff cannot use oneAccess (see the list of scenarios under the "Apply for Access to MiSiS" section) use one of the following MiSiS Access Request Forms:

  - MiSiS Access Request Form for Region & Central Office Staff

- To remove access from a batch of employees, submit the:
  Removing MiSiS Access from Former Employees Fax Form

## *District Bulletins on Information Security*

The following bulletins provide policy information on access to student information.

BUL-999.15 Responsible Use Policy

This revision replaces BUL-999.14, dated September 25, 2023. It was revised to address the use of artificial intelligence (AI) tools, including generative artificial intelligence tools, which can generate new content including text, images, video, audio, structures, computer code, synthetic data etc. in response to prompts from users. This version also includes an acknowledgement of receipt and use of District owned devices.

BUL-1077.2 Information Protection Policy

The purpose of this bulletin is to define the requirements for maintaining security of information within and outside the District. As a public institution, much of the information possessed by the District is a matter of public record. However, there are types of information that require care and sensitivity in handling, such as student education records, employee personnel records, and health care records. This bulletin also addresses data ownership and responsibilities of data owners.

BUL-6887.1 Pupil Records: Access, Confidentiality, and Notice of Educational Rights

This bulletin establishes policy and procedures for compliance with confidentiality and privacy provisions regarding pupil record information.