# Student Management System

## User Security

NY State Comptrollers Audit Report

- Who authorizes the assignment of user rights in your district's student management system?
- Who in your district is responsible to make the appropriate approved changes to the user rights in your district's student management system?
- Are these changes documented?
- Why is it important?

# Audit - From the office of NY State Comptroller
# Access  Controls Over Student Information Systems

## *"Schools Must Do More to Limit Access to Sensitive Student Databases"*

Audit Results of six school districts in central and northern NY.  "The objective…whether districts adequately control access to their SIS system."

"The districts that we reviewed did not adequately control access to SIS."

"None of the districts adopted comprehensive (written) user access policies and procedures, increasing the risk that PPSI could be accessed, changed or misused by unauthorized persons."

"Our tests of 229 SIS users found that 90 users (39 percent) had access to one or more functions even though it was not their job responsibility to perform those functions."

" We also found that none of the districts reviewed audit logs or change reports for potentially unauthorized changes. When audit logs or change reports are not generated and reviewed, officials cannot be assured that unauthorized activities, such as improper grade changes, are detected and adequately addressed."

“All six districts have policies limiting access to only authorized district personnel and breach notification policies that detail how district employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired without valid authorization. ***However, none of the districts adopted comprehensive written policies and procedures addressing user access issues such as adding, deactivating or modifying user rights and accounts.”***

“As a result of control weaknesses at each district, we found that certain users were assigned more rights than needed for their job duties. Without written procedures for staff responsible for the maintenance of user accounts and monitoring access rights, there is an increased risk that rights will be assigned incorrectly and that access to SIS will not be properly restricted.”

# SIS Functions that were Audited

- Grade Changes
- View/Modify Health Records
- Change Student Demographic Information
- Add Staff User Account
- Assume Identity Feature
- Assume Account Feature

# Recommendations made:

1. Establish written policies and procedures for SIS administration including a formal authorization process to add, deactivate or change user accounts and rights and procedures for monitoring user access.
2. Review current procedures for assigning user access rights and strengthen controls to ensure that individuals are assigned only those access rights needed to perform their job duties and should monitor user access rights periodically,
3. Evaluate user rights and permissions currently assigned to each SIS user, including RIC employees and vendors, and ensure that rights are updated as needed to properly restrict access,
4. Restrict the ability to make grade changes to designated individuals and ensure that documentation is retained to show who authorized the grade changes and the reasons for the changes,

# Recommendations continued

1. Remove all unknown and generic or shared SIS accounts and deactivate the accounts of any users who are no longer employed,
2. Determine whether the assume-identity and assume-account features are appropriate for use (if currently available); if these features are used, district officials must strictly control access and review SIS data that clearly shows user activity performed and all accounts involved when these features are used, and
3. Periodically review available audit logs for unusual or inappropriate activity. If useful audit logs are currently not available, District officials should work with their SIS provider to determine if useful logs or change reports can be generated to monitor activities.

## Some questions asked.

- Who are the designated SIS administrators?  List names, titles, and job description of all designated SIS administrators.
- Do any other users have full access rights to the SIS  If yes, list the names, titles, job descriptions and the reasons for them needing these rights.
- Are user accounts periodically reviewed to see who has access to the SIS and which users might have unnecessary privileges?  If yes, how often are they reviewed?
- What standards, procedures, and/or forms are used in the process to add, delete or modify an individual's access rights to the SIS?  Provide any written documentation you have related to this.

**Eastern Suffolk BOCES Board and Administration**

**President**
Lisa Israel

**Vice President**
William K. Miller

**Member and Clerk**
Fred Langstaff

**Members**

Arlene Barresi
Walter Wm. Denzler, Jr.
Stephen L. Gessner, Ph.D.
Linda S. Goldsmith
William Hsiang
Susan Lipman
Joseph LoSchiavo
Anne Mackesey
James F. McKenna
Brian O. Mealy
Catherine M. Romano
John Wyche

**District Superintendent**
David Wicks

**Chief Operating Officer**
Julie Davis Lutz, Ph.D.

**Associate Superintendent**
Ryan J. Ruf - Management Services

**Associate Superintendent**
Peggie Staib, Ed.D. - Educational Services

**Assistant Superintendent**
R. Terri McSweeney, Ed.D. - Human Resources

**Directors**
Keith Anderson - Building Services
Leah Arnold - Career, Technical and Adult Education
Kate Davern - Education and Information Support Services
Colleen Lippoper - Business Services
Susan Maddi - Administrative Services
Grant Nelsen - Technology Integration
Gina Reilly - Special Education
Darlene Roces - Regional Information Center

**www.esboces.org**