



STATE OF ILLINOIS
**OFFICE OF THE
 AUDITOR GENERAL**

Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

ILLINOIS MATHEMATICS & SCIENCE ACADEMY

State Compliance Examination
 For the Year Ended June 30, 2022

Release Date: February 2, 2023

FINDINGS THIS AUDIT: 3	New	Repeat	Total	AGING SCHEDULE OF REPEATED FINDINGS			
				Repeated Since	Category 1	Category 2	Category 3
Category 1:	0	0	0	2021		22-01, 22-02	
Category 2:	1	2	3				
Category 3:	0	0	0				
TOTAL	1	2	3				
FINDINGS LAST AUDIT: 4							

INTRODUCTION

The Illinois Mathematics and Science Academy (Academy) develops creative, ethical leaders in science, technology, engineering and mathematics. As a teaching and learning laboratory created by the State of Illinois, the Academy enrolls academically talented Illinois students (grades 10-12) in its advanced, residential college preparatory program, and it serves thousands of educators and students in Illinois and beyond through innovative instructional programs that foster imagination and inquiry

SYNOPSIS

- (22-01) The Academy had not implemented adequate internal controls related to cybersecurity programs, practices and control of confidential information.

Category 1:	Findings that are material weaknesses in internal control and/or a qualification on compliance with State laws and regulations (material noncompliance).
Category 2:	Findings that are significant deficiencies in internal control and noncompliance with State laws and regulations.
Category 3:	Findings that have no internal control issues but are in noncompliance with State laws and regulations.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Weaknesses in Cybersecurity Programs and Practices

The (Academy) had not implemented adequate internal controls related to cybersecurity programs, practices and control of confidential information.

To assist the Academy in meeting its mission of providing education to high school individuals, the Academy utilizes information technology applications which contain confidential information and personal information.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the Academy's cybersecurity program, practices and control of confidential information, we noted the Academy had not:

Academy had not fully developed its cybersecurity programs, practices and control of confidential information

- Developed a formal, comprehensive, adequate, and communicated security program (including policies, procedures, and processes as well as clearly defined responsibilities over the security of computer programs and data) to manage and monitor the regulatory, legal, environmental and operational requirements.
- Developed policies and procedures for reporting security violations and suspected violations.
- Developed a cybersecurity plan.
- Developed a project management framework to ensure new applications were adequately developed and implemented in accordance with management's expectations.
- Ensured assets were monitored to identify security events, the impact, and the follow-up actions taken.
- Developed a risk management methodology, conducted a comprehensive risk assessment, or implemented risk reducing internal controls.
- Required employees to annually acknowledge receipt of obtaining and understanding the security policies.
- Developed a data classification methodology and classified its data to identify and ensure adequate protection of information.
- Required contractors to acknowledge receipt and understanding of the security policies.
- Required contractors to complete cybersecurity training.
- Required electronic media to be encrypted (Finding 01, pages 8-10).

Academy did not require contractors to acknowledge receipt and understanding of policies or complete cybersecurity training

We recommended the Academy:

- Develop a formal, comprehensive, adequate, and communicated security program to manage and monitor the regulatory, legal, environmental and operational requirements.
- Develop policies and procedures for reporting security violations and suspected violations.
- Develop a cybersecurity plan describing the security program, policies and procedures.
- Develop a project management framework to ensure new applications are adequately developed and implemented in accordance with management's expectations.
- Ensure assets are monitored to identify security events, the impact, frequency of reviews and follow-up actions taken.
- Develop a risk management methodology, conduct a comprehensive risk assessment, and implement risk reducing internal controls.
- Require employees to annually acknowledge receipt and understanding of the security policies
- Develop a data classification methodology, classify its data to identify and ensure adequate protection of information.
- Require contractors to acknowledge receipt and understanding of the security policies.
- Require contractors to complete cybersecurity training.
- Require electronic media to be encrypted

Academy agreed

The Academy agreed with the recommendations and stated they will work on establishing a more formalized and comprehensive program.

OTHER FINDINGS

The remaining findings pertain to the Academy's Disaster Recovery Plan and performance evaluations. We will review the Academy's progress towards the implementation of our recommendations in our next State compliance examination.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the Academy for the year ended June 30, 2022, as required by the Illinois State Auditing Act. The accountants stated the Academy complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by Borschnack, Pelletier & Co.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:JGR