AUDITORS' REPORT

STATE DATA CENTER GENERAL CONTROLS

Eastern Connecticut State University

AS OF OCTOBER 2023

STATE OF CONNECTICUT
Auditors of Public Accounts

JOHN C. GERAGOSIAN
State Auditor

CRAIG A. MINER
State Auditor

CONTENTS

STATE OF CONNECTICUT

AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

STATE CAPITOL
210 CAPITOL AVENUE
HARTFORD, CONNECTICUT 06106-1559

CRAIG A. MINER

April 7, 2026

INTRODUCTION

We are pleased to submit this state data center general controls audit of Eastern Connecticut State University as of October 2023 in accordance with the provisions of Section 2-90 of the Connecticut General Statutes. Our audit identified internal control deficiencies; instances of noncompliance with laws, regulations, or policies; and a need for improvement in practices and procedures that warrant management's attention.

The Auditors of Public Accounts wish to express our appreciation for the courtesies and cooperation extended to our representatives by the personnel of Eastern Connecticut State University during the course of our examination.

The Auditors of Public Accounts also would like to acknowledge the auditors who contributed to this report:

Christopher D'Amico
Gavin Davids
Dennis Howard

Christopher D'Amico
Principal Auditor

Approved:

John C. Geragosian
State Auditor

Craig A Miner
State Auditor

AUDIT-AT-A-GLANCE

Category	Description
Maintenance	Maintenance controls concern how well agencies keep their information technology (IT) systems up to date, patched, and operational. The university should ensure maintenance records are appropriately recorded and reviewed. (See Finding 5.)
Personnel	Personnel controls identify how well IT groups are staffed, aware of their responsibilities, and able to perform their duties. This engagement did not note any related findings or recommendations.
Planning	Planning controls indicate how well IT systems are insulated from disruption, unauthorized access, and similar events that might detrimentally impact operations. The university should develop a local response to IT related incidents and train staff on disaster recovery procedures. (See Findings 1 and 4.)
Security	Security controls identify how well IT systems are protected (physically and logically) and ensure an entity's data are backed up and accessible. The university should ensure that access to restricted areas is physically protected and provided only to appropriate personnel. (See Findings 2 and 3.)

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our examination of Eastern Connecticut State University state data center general controls disclosed the following five recommendations, which were not repeated from the previous audit.

Finding 1

Incident Response Deficiencies (Planning)

Criteria

The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends development of an incident response plan to mitigate the impact of an attack, correct vulnerabilities, and secure the overall organization in a coordinated manner.

In addition, entities relying on a service organization to provide critical infrastructure, services, or other operations should regularly obtain and review a Service and Organizational Control (SOC) I or II report. The SOC report is intended to provide an independent, third-party verification that a service organization has appropriate controls and safeguards to protect client data and ensure operational integrity.

Condition

The university could not provide complete incident response documentation for its or its third-party service provider's activities.

Context

We requested documentation of the university's incident response activities, such as a high-level plan or third-party assurance of their incident response vendor.

Effect

Deficiencies in an incident response plan can increase risk of interruptions to business operations. Furthermore, without reviewing a vendor's SOC report, an entity could be accepting more risk that the vendor lacks adequate and sufficient internal controls.

Cause

There appears to be a lack of management oversight.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

Eastern Connecticut State University should ensure it has complete incident response documentation.

Agency Response

"We agree with this recommendation. An Incident Response Plan was created in June 2024. We are reviewing the 2024 plan to further mature and expand our IR documentation. We are targeting October 2026 to complete the review process."

Finding 2

Physical Security of Data Centers (Security)

Criteria

The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends tracking and limiting physical access to data centers to reduce the likelihood of unauthorized access.

Condition

During a walkthrough of the facility, we noted that the university did not secure a sensitive IT area.

Context

Physical locks and card readers should protect sensitive IT areas from unauthorized access.

Effect

Failing to physically secure sensitive IT areas increases risk to business operations.

Cause

ECSU management indicated that a vendor performing authorized work circumvented controls over the limited access area.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

Eastern Connecticut State University should ensure established controls over information technology physical security are operating as intended and are not circumvented without compensating controls in place.

Agency Response

"We agree with this recommendation and ECSU took immediate corrective action to address this concern. The vendor was notified of the requirement to follow proper data center and network closet security protocols, specifically identifying breach of physical security that occurred by propping open doors and leaving them unattended. Going forward, all new vendors who have access to secure areas are notified of our protocols."

Finding 3
Oversight of Authorized Access to Data Centers (Security)

Criteria

The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends establishing criteria for authorizing access to data centers, with approval and regular access reviews by management.

Condition

The university's data center access procedures do not include an appropriate approval process for granting access to sensitive IT areas.

Context

We reviewed the university's data center access procedures.

Effect

Individuals with no functional necessity could be granted access to sensitive IT areas, increasing risk of unintended modification or damage to physical IT resources stored in sensitive IT areas.

Cause

Lack of sufficient procedures appears to be due to a lack of management oversight.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

Eastern Connecticut State University should update its procedures to ensure that access to sensitive information technology areas is restricted to those who require access to perform their job duties and regular access reviews.

Agency Response

"We agree with this recommendation and have successfully implemented a new electronic door access system to enhance physical security and oversight. This system provides the granular control and reporting capabilities necessary to restrict access to sensitive IT areas based on job function. To ensure these controls remain effective, ECSU has established a formal review protocol requiring access lists to be audited at least three times per year (once per academic semester) by the CIO or designee. The review process ensures that permissions are kept current and that any unauthorized or obsolete access is promptly revoked."

Finding 4
Contingency Planning Training (Planning)

Criteria

The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends that appropriate organizational personnel should be trained on contingency plans to allow them to better handle disaster recovery events.

Condition

The university was unable to provide documentation that it trained its IT employees on contingency planning.

Context

We requested documentation showing that university IT employees completed contingency planning training and relevant training materials.

Effect

Lack of training increases the time required to recover from an incident and return to stable operation when an organization must activate a contingency plan.

Cause

The condition appears to be due to lack of management oversight.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

Eastern Connecticut State University should ensure appropriate personnel are trained on all aspects of contingency and disaster recovery. The university should ensure that training materials are readily available to authorized personnel in the event of a contingency plan activation.

Agency Response

"We agree with this recommendation and have significantly expanded our disaster recovery (DR) training program. Throughout 2025 and early 2026, key personnel participated in multiple tabletop exercises, including sessions led by ECSU Public Safety on May 5 and October 10, 2025, and an exercise on March 19, 2025 held by Central Connecticut State University. Additionally, university leadership reviewed our campus wide Emergency Action Plan on February 4, 2026. Starting in the Fall, Technology Services will be conducting internal tabletop exercises each semester specifically targeted toward testing our revised IR Plan and recovery procedures."

Finding 5
Deficiencies in Data Center Maintenance (Maintenance)

Criteria

The National Institute of Standards and Technology (NIST) Special Publication 800-53 recommends that maintenance logs for information technology equipment are utilized and reviewed.

Condition

The university could not provide appropriate information technology equipment maintenance logs upon our request. In addition, the university did not keep current fire suppression system maintenance logs.

Context

We requested all relevant physical maintenance logs, which might include systems such as power, climate control, and fire suppression. The university only provided the fire suppression system maintenance log.

Effect

When an agency lacks maintenance logs, there is less assurance that it performed regular maintenance on critical IT infrastructure and devices. There is also less accountability that the university's IT employees conducted required maintenance.

Cause

The condition appears to be due to lack of management oversight.

Prior Audit Finding

This finding has not been previously reported.

Recommendation

Eastern Connecticut State University should strengthen internal controls by logging and reviewing its information technology maintenance activities.

Agency Response

"We agree with the recommendation to strengthen internal controls over information technology maintenance logging and reviews. While Facilities was made aware of this finding at the time, leadership in Facilities and Technology Services has changed since then. The CIO and the Assistant VP for Facilities will meet regarding this finding and reaffirm the need for proper logging and the protocols to be followed. This meeting will happen before the end of the Spring 2026 semester."

OBJECTIVES, SCOPE, AND METHODOLOGY

We have audited certain operations of Eastern Connecticut State University in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to, university data center general controls as of October 2023. The objectives of our audit were to evaluate the:

1. University's internal controls over significant information technology resources;

2. University's compliance with policies and procedures internal to the university or promulgated by other state agencies; and

3. Effectiveness and efficiency of certain management practices and operations.

Our methodology included reviewing written policies and procedures and other pertinent documents; interviewing various personnel of the university, and testing selected transactions. Our testing was not designed to project to a population unless specifically stated. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We tested internal controls using the National Institute of Standards and Technology's (NIST) Special Publication 800-53 – "Security and Privacy Controls for Information Systems and Organizations" as a guide. This publication includes internal controls that provide a comprehensive foundation for an organization's information security. We used this publication to plan the audit testing performed for this engagement.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The accompanying agency overview is presented for informational purposes. This information was obtained from various available sources including, but not limited to, the university's management and the state's information systems, and was not subjected to the procedures applied in our audit of the university. For the areas audited, we identified

1. Deficiencies in internal controls;

2. Apparent noncompliance with laws, regulations, contracts and grant agreements, policies, or procedures; and

3. A need for improvement in management practices and procedures that we deemed to be reportable.

The State Auditors' Findings and Recommendations section of this report presents findings arising from our audit of Eastern Connecticut State University. Due to the sensitive nature of the information technology environment, certain confidential portions of this report and its findings have been omitted to prevent unintentional disclosure of sensitive information. Details of our findings have been provided to university management for corrective action in a separate communication, which along with its supporting workpapers, are not subject to public disclosure in accordance with Sections 1-210(b)(20) and 2-90(h) of the General Statutes.

ABOUT THE AGENCY

Audit Purpose

We conducted this audit to obtain an understanding of Eastern Connecticut State University's data center and its information systems and data. Our review was intended to: (1) identify the design and implementation of the university's information technology general controls, (2) assess and evaluate those controls and practices against industry standards and state policies and procedures, and (3) identify and communicate opportunities for improvement in the university's IT control environment.

Agency Overview

Eastern Connecticut State University in Willimantic is one of the four higher education institutions that collectively make up the Connecticut State University component of the Connecticut State Colleges and Universities System. The Board of Regents for Higher Education, which serves as the administrative office for CSCU, oversees the university.

The information technology group at Eastern Connecticut State University supports and oversees all of the technological needs of the university. This includes networking and communication, computers and labs, and the school's data center. The IT group also administers user accounts and related needs for connecting to the Banner information system. Overall, this group represents a critical aspect of the university's ongoing operations.