

Audit Report

**University System of Maryland
Salisbury University**

May 2015



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

**Department of Legislative Services
Office of Legislative Audits**

301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Phone: 410-946-5900 · 301-970-5900

Toll Free in Maryland: 1-877-486-9964

Maryland Relay: 711

TTY: 410-946-5401 · 301-970-5401

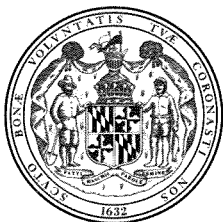
E-mail: OLAWebmaster@ola.state.md.us

Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website:



The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

May 6, 2015

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate Craig J. Zucker, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the University System of Maryland (USM) – Salisbury University (SU) for the period beginning July 1, 2011 and ending September 8, 2014. SU is a comprehensive public institution of USM and provides a broad range of baccalaureate programs as well as selected professionally oriented master's programs and doctoral programs.

Our audit disclosed that numerous individuals had unnecessary access capabilities to process critical transactions on SU's financial management systems. In addition, controls over sensitive personally identifiable information maintained in a database and procedures for securing workstations, laptops, and servers were not sufficient. Finally, non-cash credits posted to student accounts receivable for housing were not sufficiently verified.

The USM Office's response to this audit, on behalf of SU, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by SU.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Background Information	4
Agency Responsibilities	4
Status of Findings From Preceding Audit Report	4
Findings and Recommendations	5
Information Systems Security and Control	
Finding 1 – Employee Access to Critical System Functions Was Not Adequately Restricted	5
Finding 2 – SU Stored Sensitive Personally Identifiable Information Within a Database In Clear Text	6
Finding 3 – SU’s Workstations, Laptops, and Servers Were Not Sufficiently Protected Against Malware	6
Student Accounts Receivable	
Finding 4 – SU Lacked Sufficient Controls to Ensure the Propriety of Certain Non-Cash Credit Adjustments Made to Student Accounts	7
Audit Scope, Objectives, and Methodology	9
Agency Response	Appendix

Background Information

Agency Responsibilities

Salisbury University (SU) is a comprehensive public institution of the University System of Maryland (USM) and operates under the jurisdiction of the System's Board of Regents. SU provides a broad range of baccalaureate programs as well as selected professionally oriented master's programs and doctoral programs. Student enrollment for the Fall 2014 semester totaled 8,770, including 7,997 undergraduate students and 773 graduate students. SU's budget is funded by unrestricted revenues, such as tuition and fees and a State general fund appropriation, as well as restricted revenues, such as federal grants and contracts. According to the State's accounting records, SU's revenues for fiscal year 2014 totaled approximately \$172 million, which included a State general fund appropriation of approximately \$42 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the six findings contained in our preceding audit report dated July 10, 2012. We determined that SU satisfactorily addressed these findings.

Findings and Recommendations

Information Systems Security and Control

Background

The Salisbury University (SU) Information Technology Department (ITD) manages the development, maintenance, and support of SU's information technology infrastructure including networking, telecommunications, and business information systems. ITD maintains SU's campus-wide network, supporting both administrative and academic operations. The network includes Internet connectivity, various administrative servers, and firewalls. ITD also maintains critical application systems supporting student administration, human resources, and financial management.

Finding 1

Employee access to critical functions on SU's financial management systems was not adequately restricted.

Analysis

SU did not adequately restrict employee access capabilities for critical functions on its financial management systems. Our review of system capabilities assigned to 149 active users disclosed that numerous users were assigned unnecessary or inappropriate access capabilities.

- Sixty users had the capability to add or update student residency information used to determine tuition rates even though these users did not require such access to perform their assigned job duties.
- Eight users had unnecessary access to add or adjust personnel and payroll data, such as pay rates and leave balances, and one of these employees could also approve certain of these adjustments.
- Two users had unnecessary access to adjust federal financial aid application data, and one of these employees had access to change the status of an application so that it would not be subject to subsequent verification.

The University System of Maryland (USM) *IT Security Standards* specify that institutions are responsible for ensuring that access rights reflect employee status, including changes in employee status. In addition, institutions must segregate functions to ensure the appropriate separation of duties for system users.

Recommendation 1

We recommend that SU restrict user access capabilities for critical functions to those employees who require such capabilities to perform their assigned job duties and in a manner that ensures a proper segregation of duties.

Finding 2

SU stored sensitive personally identifiable information within a database in clear text.

Analysis

SU stored sensitive personally identifiable information (PII) within a database in clear text. Specifically, we determined that SU stored PII including social security numbers, full names, and dates of birth in clear text in one of its databases.

As of October 29, 2014, based on our inquiry, SU personnel identified approximately 294,000 unique social security numbers along with related full names and dates of birth which were not encrypted. This sensitive PII, which is commonly sought by criminals for use in identity theft, should be protected by appropriate information system security controls. The *USM IT Security Standards* state that USM institutions must utilize encryption for confidential data.

Recommendation 2

We recommend that SU encrypt all database tables containing sensitive PII in accordance with the *USM IT Security Standards*.

Finding 3

SU's workstations, laptops, and servers were not sufficiently protected against malware.

Analysis

SU's workstations, laptops, and servers were not sufficiently protected against malware.

- SU did not restrict the use of administrator rights on its workstations to network administrators. Rather, we determined that 711 unique users had local administrator rights on 983 of SU's 3,400 workstations. Administrator rights are the highest permission level that can be granted to users and it allows users to install software and change configuration settings. As a result,

if these workstations were infected with malware, the malware would run with administrator rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights. In addition, users with administrative rights can disable the anti-malware software on their workstations.

- We were advised by SU personnel that a host-based firewall was not enabled on any SU laptops. Therefore, when these laptops were used outside of the SU network they were susceptible to attack from untrusted traffic. According to SU records, as of February 4, 2015 there were 422 SU-owned laptops in use.
- Anti-malware software was not installed on any of SU's 216 servers. As a result, these servers were more susceptible to malware exploits.

The USM *IT Security Standards* state that institutions must implement and document processes that minimize provisioning of local administrative rights so that only those employees who require it are given those rights. Additionally, these *Standards* state that institutions must protect against malicious code by implementing solutions that, to the extent possible, include a capability for automatic updates.

Recommendation 3

We recommend that SU

- a. restrict administrative rights on workstations to network administrators,**
- b. ensure that all laptop computers are protected by a properly configured and enabled host-based firewall, and**
- c. ensure that anti-malware software is installed on all SU servers.**

Student Accounts Receivable

Finding 4

SU lacked sufficient controls to ensure the propriety of certain non-cash credit adjustments made to student accounts.

Analysis

SU had not established adequate controls over the processing of non-cash credit adjustments related to student housing. These adjustments may be required when, for example, a student withdraws from SU or requests a change in housing. Although an output report of all non-cash credit adjustments recorded in student accounts was periodically generated and reviewed on a test basis by an

independent employee, any housing-related adjustments selected for review during this procedure were not verified to appropriate source documentation, such as an approved housing cancellation form. As a result, there was a lack of assurance that only valid adjustments were processed. According to SU's records, non-cash credit adjustments processed in fiscal year 2014 relating to housing totaled approximately \$1 million.

Recommendation 4

We recommend that SU ensure that non-cash credit adjustments posted to student accounts related to housing charges are verified to appropriate source documents.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the University System of Maryland (USM) – Salisbury University (SU) for the period beginning July 1, 2011 and ending September 8, 2014. The audit was conducted 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.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine SU's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included purchases and disbursements, student accounts receivable, financial aid, cash receipts, payroll, and information technology systems. We also determined the status of the findings included in our preceding audit report.

Our audit did not include certain support services provided to SU by the USM Office. These support services (such as bond financing) are included within the scope of our audit of the USM Office. In addition, our audit did not include an evaluation of internal controls over compliance with federal laws and regulations for federal financial assistance programs and an assessment of SU's compliance with those laws and regulations because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including the components of the USM.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of SU's operations, and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were

sufficiently reliable for the purposes the data were used during this audit. We also extracted data from SU's financial systems for the purpose of testing certain areas, such as student accounts receivable and financial aid. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

SU's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect SU's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to SU that did not warrant inclusion in this report.

The response from the USM Office, on behalf of SU, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the USM Office regarding the results of our review of its response.

APPENDIX



OFFICE OF THE CHANCELLOR

May 1, 2015

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

1807
University of Maryland,
Baltimore

1856
University of Maryland,
College Park

1865
Bowie State University

1866
Towson University

1886
University of Maryland
Eastern Shore

1898
Frostburg State University

1900
Coppin State University

1925
Salisbury University

1925
University of Baltimore

1925
University of Maryland
Center for Environmental
Science

1947
University of Maryland
University College

1966
University of Maryland,
Baltimore County

Re: University System of Maryland – Salisbury University
Period of Audit: July 1, 2011 through September 8, 2014

Dear Mr. Barnickel:

I have enclosed the University System of Maryland's responses to your draft report covering the examination of the accounts and records of Salisbury University. Our comments refer to the individual items in the report.

Sincerely,

William E. Kirwan
Chancellor

Enclosures

cc: Dr. Janet Dudley-Eshbach, Ph.D, President, SU
Ms. Betty Crockett, Vice President for Administration and Finance, SU
Mr. James L. Shea, Chair, University System of Maryland Board of Regents
Mr. Anwer Hasan, Chairman, MHEC
Ms. Jennie C. Hunter-Cevera, Ph.D., Acting Secretary of Higher Education,
MHEC
Mr. Robert L. Page, Associate Vice Chancellor for Financial Affairs, USM
Office
Mr. David Mosca, Director of Internal Audit, USM Office

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
SALISBURY UNIVERSITY
JULY 1, 2011 TO SEPTEMBER 8, 2014**

Information Systems Security and Control

Finding 1

Employee access to critical functions on SU's financial management systems was not adequately restricted.

Recommendation 1

We recommend that SU restrict user access capabilities for critical functions to those employees who require such capabilities to perform their assigned job duties and in a manner that ensures a proper segregation of duties.

University response

The University agrees with this recommendation.

The financial aid access was changed to "display only" on December 5, 2014. The human resources access for the two employees no longer in HR was removed on December 15, 2014. The remaining human resources access was removed on February 12, 2015. On February 18, 2015, the residency access was removed.

We are currently working on improved security queries and reports which will focus on access to critical functions. We appreciate the help that the OLA and USM Internal Audit have provided regarding such.

Finding 2

SU stored sensitive personally identifiable information within a database in clear text.

Recommendation 2

We recommend that SU encrypt all database tables containing sensitive PII in accordance with the USM *IT Security Standards*.

University response

The University agrees with this recommendation.

On February 23, 2015, we implemented approved database encryption technology to encrypt all database objects containing sensitive personally identifiable information.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
SALISBURY UNIVERSITY
JULY 1, 2011 TO SEPTEMBER 8, 2014**

Finding 3

SU's workstations, laptops, and servers were not sufficiently protected against malware.

Recommendation 3

We recommend that SU

- a. restrict administrative rights on workstations to network administrators,**
- b. ensure that all laptop computers are protected by a properly configured and enabled host-based firewall, and**
- c. ensure that anti-malware software is installed on all SU servers.**

University response

We agree with the finding and will proceed as follows:

- a. We will complete the removal of administrative rights for all computer users by August 31, 2016. In circumstances where granting administrative rights to a computer user is warranted, an exception will be made. There will be an annual review to ensure that the reason administrative rights were initially granted still exists. Dependent upon the outcome of that review, the administrative rights will either continue or be removed.
- b. We will implement host-based firewalls on all SU maintained laptops by December 31, 2015.
- c. We will review malware and anti-virus protection solutions for traffic destined to workstations and servers. The anti-malware software will be installed by March 31, 2016.

Student Accounts Receivable

Finding 4

SU lacked sufficient controls to ensure the propriety of certain non-cash credit adjustments made to student accounts.

Recommendation 4

We recommend that SU ensure that non-cash credit adjustments posted to student accounts related to housing charges are verified to appropriate source documents.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
SALISBURY UNIVERSITY
JULY 1, 2011 TO SEPTEMBER 8, 2014**

University response

The University agrees with this recommendation.

Beginning on February 9, 2015, we began independently verifying non-cash credits for housing charges to source documents (e.g., Residence Hall Contract Cancellation form).

AUDIT TEAM

William R. Smith, CPA

Audit Manager

Richard L. Carter, CISA

Stephen P. Jersey, CPA, CISA

Information Systems Audit Managers

Ken H. Johanning, CPA, CFE

Senior Auditor

Christopher D. Jackson, CISA

Edwin L. Paul, CPA, CISA

Information Systems Senior Auditors

R. Frank Abel, CPA, CFE

Richard Tran

Staff Auditors

J. Gregory Busch

Information Systems Staff Auditor