VIRGINIA COMMONWEALTH UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of Virginia Commonwealth University (University) as of and for the year ended June 30, 2023, and issued our report thereon, dated December 11, 2023. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.vcu.edu. Our audit found:

- the financial statements are presented fairly, in all material respects; and

- two internal control findings requiring management's attention that also represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses.

Our audit also included testing over the major federal program of the Research and Development Cluster for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; and found no internal control findings requiring management's attention or instances of noncompliance in relation to this testing.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and developing and appropriately implementing adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Service Provider Oversight

Type: Internal Control and Compliance
Severity: Significant Deficiency

Virginia Commonwealth University (University) does not appropriately monitor the effectiveness of the security controls of information technology (IT) service providers (providers) in accordance with the University's adopted Information Security Standard, the International Organization for Standardization and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard), as well as the University's standards, including the University's Business Partner Security Standard. Providers are organizations that perform certain business tasks or functions on behalf of the University.

The ISO standard requires the University to implement certain controls to gain assurance over its providers and reduce the risk to the confidentiality, integrity, and availability of the University's sensitive data and information. During fiscal year 2023, the University did not review an independent audit assurance report for its enterprise resources planning system provider. Additionally, the University does not obtain and review independent audit assurance reports for the University's subservice providers. This is a result of the University's Information Security Office allocating resources to other initiatives during the year, and not having a policy or procedure that requires the assessment and documentation of the significance and risk of activities provided by subservice providers.

The Information Security Office should adhere to the University's Business Partner Security Standard and obtain and review independent audit assurance reports for all significant service providers on an annual basis. Additionally, the Information Security Office should evaluate and determine which subservice providers are significant to the University's operations. For all significant subservice providers, the University should determine the best way to obtain assurance over the relevant controls at the subservice provider and document the results of the procedures performed. This could include obtaining and reviewing independent audit assurance reports for the subservice providers. Doing so will help safeguard the confidentiality, integrity, and availability of the University's sensitive and mission critical data.

Improve Security Awareness Training

Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not meet certain requirements in the ISO Standard for security awareness training. Specifically, the University does not have an adequate process to ensure that all users complete security awareness training, and the University does not provide role-based training to users with specific information security roles and responsibilities. An established security awareness and training program is essential to protecting University IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the University. Our review of the University's security awareness and training program identified the following weaknesses:

- 974 of 8,063 (12%) users did not complete security awareness training within the past year. The ISO Standard requires that personnel should annually receive appropriate information security awareness, education, and training as relevant for their job function (*ISO 27002 Section: 6.3*).

- The University does not provide role-based training to all users with designated security roles, such as system owners, data owners, system administrators, and security personnel. The University's Personnel Standard requires that all applicable individuals must complete role-specific security awareness training. Additionally, the ISO Standard requires the implementation of an appropriate training plan for technical teams whose roles require specific skill sets and expertise (*ISO 27002 Section: 6.3*).

The University does not use an enforcement measure that forces users to complete training, such as disabling a user's account until training is complete. Without a process to ensure that all users receive security awareness training annually, the University increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

The University's Personnel Standard does not define the personnel with assigned security-based roles and responsibilities that must take role-specific training and does not define the specific training that each role should take. Lack of adequate role-based training increases the risk that users will be unaware or lack pertinent skills and knowledge to perform their security related functions, increasing the risk to sensitive data.

The University should improve their security awareness and training program to include an enforcement measure to ensure that all employees complete the training before accessing computer resources and on an annual basis thereafter. Additionally, the University should develop a formal process to provide role-based training to users with designated security roles. Improving the security awareness and training program will help protect the University from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 11, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Virginia Commonwealth University

President Michael Rao
Virginia Commonwealth University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **Virginia Commonwealth University** as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated December 11, 2023. Our report includes a reference to other auditors who audited the financial statements of the component units of the University, as described in our report on the University's financial statements. The other auditors, excluding those of Dentistry@VCU, did not audit the financial statements of the component units of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with those component units of the University. Additionally, this report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters for Dentistry@VCU, that are reported on separately by those auditors.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve IT Service Provider Oversight" and "Improve Security Awareness Training," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings titled "Improve IT Service Provider Oversight" and "Improve Security Awareness Training."

The University's Response to Findings

We discussed this report with management at an exit conference held on December 5, 2023. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the findings identified in our audit, which is included in the accompanying section titled "University Response." The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The University has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JMR/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Improve IT Asset Management Process	Complete	2022
Improve Firewall Security	Complete	2022
Improve IT Change Management Procedures and Process	Complete	2022
Improve IT Service Provider Oversight	Ongoing	2023
Improve Security Awareness Training	Ongoing	2023

January 8, 2024

Patricia Perkins
AVP of Finance and University Controller

912 West Franklin Street
Box 842035
Richmond, Virginia 23284-2512

804 828-5474

Staci Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2023 audit by the Auditor of Public Accounts and discussed during the exit conference.

Improve Information Technology Service Provider Oversight

Virginia Commonwealth University (University) does not appropriately monitor the effectiveness of the security controls of information technology (IT) service providers (providers) in accordance with the University's adopted Information Security Standard, the International Organization for Standardization and the International Electrotechnical Commission Standard ISO/IEC 27002 (ISO Standard), as well as the University's standards, including the University's Business Partner Security Standard. Providers are organizations that perform certain business tasks or functions on behalf of the University.

The ISO standard requires the University to implement certain controls to gain assurance over its providers and reduce the risk to the confidentiality, integrity, and availability of the University's sensitive data and information. During fiscal year 2023, the University did not review an independent audit assurance report for its enterprise resources planning system provider. Additionally, the University does not obtain and review independent audit assurance reports for the University's subservice providers. This is a result of the University's Information Security Office allocating resources to other initiatives during the year, and not having a policy or procedure that requires the assessment and documentation of the significance and risk of activities provided by subservice providers.

The Information Security Office should adhere to the University's Business Partner Security Standard and obtain and review independent audit assurance reports for all significant service providers on an annual basis. Additionally, the Information Security Office should evaluate and determine which subservice providers are significant to the University's operations. For all significant subservice providers, the University should determine the best way to obtain assurance over the relevant controls at the subservice provider and document the results of the

procedures performed. This could include obtaining and reviewing independent audit assurance reports for the subservice providers. Doing so will help safeguard the confidentiality, integrity, and availability of the University's sensitive and mission critical data.

VCU Response:

VCU will adhere to its standards and procedures to ensure the annual review of assurance documentation for its core service providers. The university will also evaluate and determine which subservice providers are significant to the University's operations. The university will attempt to obtain additional third-party attestation or alternative documentation for these sub-service providers, evaluate them if they are made available through the service providers, and document the results of the procedures performed.

Responsible Person: Dan Han, Chief Information Security Officer

Completion Date: June 30, 2024

Improve Security Awareness Training

The University does not meet certain requirements in the ISO Standard for security awareness training. Specifically, the University does not have an adequate process to ensure that all users complete security awareness training, and the University does not provide role-based training to users with specific information security roles and responsibilities. An established security awareness and training program is essential to protecting University IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the University. Our review of the University's security awareness and training program identified the following weaknesses:

- 974 of 8,063 (12%) users did not complete security awareness training within the past year. The ISO Standard requires that personnel should receive appropriate information security awareness, education, and training as relevant for their job function (ISO 27002 section: 6.3).

- The University does not provide role-based training to all users with designated security roles, such as System Owners, Data Owners, System Administrators, and security personnel. The University's Personnel Standard requires that all applicable individuals must complete role- specific security awareness training. Additionally, the ISO Standard requires the implementation of an appropriate training plan for technical teams whose roles require specific skill sets and expertise (ISO 27002 section: 6.3).

The University does not use an enforcement measure that forces users to complete the training, such as disabling a user's account until training is complete. Without a process to ensure

that all users receive security awareness training annually, the University increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

The University's Personnel Standard does not define the personnel with assigned security- based roles and responsibilities that must take role-specific training and does not define the specific training that each role should take. Lack of adequate role-based training increases the risk that users will be unaware or lack pertinent skills and knowledge to perform their security related functions, increasing the risk to sensitive data.

The University should improve their security awareness and training program to include an enforcement measure to ensure that all employees complete the training before accessing computer resources and on an annual basis thereafter. Additionally, the University should develop a formal process to provide role-based training to users with designated security roles. Improving the security awareness and training program will help protect the University from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

VCU Response:

VCU is actively revising how mandatory training is being managed and will identify methods to place consequences on individuals who fail to complete the required training. Additionally, VCU will implement a mandatory annual role-based training with associated tracking for its IT staff.
.
Responsible Person: Dan Han, Chief Information Security Officer

Completion Date: June 30, 2024

Sincerely,

DocuSigned by:
Patricia Perkins
AB2B6C352A2449B...

Patricia Perkins
Associate VP of Finance and University Controller
Virginia Commonwealth University