RADFORD 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 Radford University (University) as of and for the year ended June 30, 2023, and issued our report thereon, dated June 5, 2024. 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.radford.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses;
- instances of noncompliance or other matters required to be reported under Government Auditing Standards; and
- the University has not completed corrective action with respect to the prior audit finding as reflected in the Findings Summary included in the Appendix.

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 develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

We did not perform audit work on the prior audit findings titled "Improve Compliance over Enrollment Reporting" and "Promptly Return Unclaimed Aid to the Department of Education" as noted in the Findings Summary included in the Appendix because the University did not implement corrective action during our audit period. Corrective action has been ongoing since the fiscal year 2018 and 2021 audits, respectively. We will follow up on these findings during the fiscal year 2024 audit.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Dedicate Additional Resources to Financial Reporting
Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2022
Prior Title: Improve Financial Reporting Review Process

Radford University (University) has made progress but continues to implement corrective actions to improve internal controls over the financial reporting process for the University's Annual Financial Report (Annual Report). Specifically, the Controller's Office performed extensive research, submitted technical inquiries, and proactively developed procedures to address new accounting standards and other complex financial events. The Controller's Office also performed a more thorough comparative analysis between current and prior year Annual Reports to identify and investigate unusual or unexpected financial activity.

Although the University made progress in addressing the prior year finding, increasing complexity of accounting standards coupled with turnover in key positions has put significant stress on the Controller's Office. As a result, the University processed the following adjustments to the Annual Report in response to our audit to ensure the fair presentation of information in accordance with generally accepted accounting principles (GAAP):

Financial Statements

- Reclassified $56.5 million in appropriations available from current assets to non-current assets within the Statement of Net Position related to unspent capital appropriations from the Commonwealth's general fund.

- Reclassified $6 million in cash inflows and outflows to non-cash activities within the Statement of Cash Flows resulting from accounting for subscription-based information technology assets.

- Reclassified $2.9 million in revenues from operating revenues to non-operating revenues within the Statement of Revenues, Expenses, and Changes in Net Position relating to the University's proportionate share of special one-time contributions from the Commonwealth to the Virginia Retirement System.

- Reclassified $839 thousand between the current and non-current portions of other noncurrent liabilities.

Footnotes

- Added $23.5 million in contractual commitments to Note 15 relating to new construction commitments for the Center for Adaptive Innovation construction project.

- Reclassified $7.3 million in auxiliary revenues within Note 11 related to the University not properly linking a supporting workbook to the Annual Report preparation software.

- Reduced $1.5 million in future interest payments on long-term debt reported within Note 7 due to the University not initially updating the schedule reported in the prior Annual Report.

Required Supplementary Information

- Made several adjustments to the Schedule of University's Share of OPEB Liability (Asset) related to the University not updating some aspects of the schedule for the current year through its Annual Report preparation software.

University management is responsible for designing and maintaining a system of internal controls relevant to the preparation and fair presentation of financial statements that are free from material misstatement in accordance with GAAP. While most of the misstatements were related to misclassifications among financial statement line items and did not have a significant impact on overall net position (0.2 percent change), misstatements of this nature can increase the risk that users will draw improper conclusions about the University's financial activities.

The Controller's Office should continue to evaluate and enhance its risk assessment and review processes over financial reporting to reduce misstatements in the University's Annual Report. The University is currently in the process of evaluating and filling vacancies in key positions within the Controller's Office and throughout the University. Management should continue these efforts and dedicate the necessary resources to support the Controller's Office and other key areas in addressing the increasing complexity of accounting standards.

Improve Timeliness of Bank Reconciliations
Type: Internal Control
Severity: Significant Deficiency

During fiscal year 2023, the University did not perform a timely year-end bank reconciliation. Specifically, the University did not fully complete its preparation or review of the June 2023 General Fund reconciliation until December 2023. As a result of delays in completing the June reconciliation, the University submitted its May General Fund cash balance to the Department of Accounts (Accounts) for inclusion in the Commonwealth's Annual Comprehensive Financial Report.

Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 20905 requires agencies to take sufficient actions to ensure that the Commonwealth's accounting system final close data is complete, correct, and in accordance with all applicable state laws and regulations. University

bank reconciliation procedures require the monthly reconciliation of all bank statements to the University's accounting system by the end of the following month.

Bank reconciliations are critical to the University's system of internal controls. Untimely preparation or review of bank reconciliations increases the risk that the University will not detect and address fraud or errors in a timely manner. Additionally, the University's decision to submit the May 2023 General Fund cash balance to Accounts resulted in Accounts using a cash balance overstated by $7.1 million. Reporting unreconciled or outdated balances increases the risk of material misstatement in the Commonwealth's Annual Comprehensive Financial Report and the University's financial statements.

Turnover in the responsible position coupled with inadequate written policies and procedures contributed to delays in completing the reconciliation. In the absence of a policy on tolerable year-end reconciling differences, the Controller's Office elected to submit the most recent reconciled cash balance to Accounts.

The University should provide adequate training and resources, including written desk procedures, for responsible individuals to ensure they properly prepare and review bank reconciliations in a timely manner and in accordance with University policies and procedures. Additionally, to the extent there may be unreconciled year-end differences in cash balances in the future, the Controller's Office should consider its policy on when it is appropriate to default to a prior period cash balance.

Improve IT Risk Management and Contingency Planning Documentation

Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not document some aspects of its information technology (IT) Risk Management and Contingency Planning in accordance with the University's IT Security Standard (University Standard) and the International Organization for Standardization and the International Electrotechnical Commission Standard, ISO/IEC 27002 (ISO Standard). IT Risk Management and Contingency Planning is critical to supporting the University's business functions and recovering IT systems when they become unavailable. Specifically, the University does not meet the following minimum requirements of the University Standard:

- The University does not test its IT Disaster Recovery Strategy (DRS) annually or Disaster Recovery Plans (DRP) every three years. The University Standard requires the University to annually review, reassess, test, and revise the IT DRS to reflect changes in the University's IT environment. The University Standard also requires the University to conduct a Disaster Recovery exercise of essential systems to assess their adequacy and effectiveness at least every three years. By not testing its IT DRS and system DRPs according to organizational requirements, the University increases the risk of having outdated disaster recovery procedures as well as extended periods of downtime, which can be costly to the University. The University experienced turnover within its IT Infrastructure department, causing a delay to perform a test of its IT DRS and DRPs (*University Standard, sections: 3.2 Continuity of*

Operations Planning, 3.3 IT Disaster Recovery Planning; ISO Standard, section: 5.30 ICT readiness for business continuity).

- The University did not accurately document the sensitivity category of confidentiality, integrity, or availability for seven out of 107 sensitive systems. The University assigns the category based on the data stored and processed by each system. The University Standard requires the data owner to determine the potential damages to the University in the event of compromise to the confidentiality, integrity, and availability of each type of data handled by the IT system and classify the sensitivity of the data accordingly. Additionally, the University's Data and System Classification Standard defines a sensitive system as one where the University rates the confidentiality, integrity, or availability as high. Although the University accurately classifies the seven systems as sensitive, inaccurate documentation of the sensitivity category could increase the risk of the University not implementing the necessary security controls to protect sensitive information or wasting unnecessary resources for non-sensitive data and systems. The University was unaware of the inaccurate documentation of data sensitivity categories for the seven systems due to recent turnover in the Information Technology Services Department, including the Information Security Officer position, which has resulted in strained resources and a lack of oversight regarding the documentation of these seven systems' sensitivity classifications (University Standard, section: 2.4 IT System and Data Sensitivity Classification; Data and System Classification Standard, sections: 2. Policy; ISO Standard, 5.12 Classification of information).

- The University does not document that it performed its scheduled review of the University Standard. The ISO Standard requires the University to review its overall information security policy and topic-specific policies at planned intervals and if significant changes occur. The University Standard specifically requires a scheduled review one year from the effective date of October 20, 2022. When performing annual reviews, the University only updates the University Standard's History section if major changes occur but has not historically determined it to be necessary to formally document its review as scheduled or to update the next planned review date. By not documenting each review of the University Standard, there is no evidence that the University is reviewing the University Standard as required. If the University does not review and revise the University Standard as required, it increases the risk that the minimum requirements defined will not align with the University's expectations and the University's current practices (University Standard, section: Preface, Scheduled Review; ISO Standard, section: 5.1 Policies for information security).

The University should dedicate the necessary resources to conduct annual IT DRS and DRP tests. The University should also re-evaluate and classify the data it stores, processes, and transmits on the University's systems based on confidentiality, integrity, and availability. The University should subsequently classify each system as sensitive or non-sensitive according to the data's sensitivity classification. Additionally, the University should document its reviews of its University Standard to indicate it performed the task. This will help ensure the University accurately identifies and evaluates risks associated with its IT environment and maintains the confidentiality, integrity, and availability of sensitive and mission-critical data.

Improve IT Asset Management
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not define certain requirements and procedures related to its IT asset management, surplus, and disposal process in accordance with the ISO Standard. Additionally, the University does not consistently follow some of the requirements and procedures outlined in the University's IT Asset Surplus Procedures (Surplus Procedures) and the University Standard. IT asset management is necessary to minimize risk and ensure proper handling and disposal of sensitive data. Specifically, the following weaknesses exist:

- The University does not enforce separation of duties by allowing the same individual to perform data removal and verify the proper removal of data from some IT assets. The University Standard states that the University shall establish separation of duties in order to protect sensitive IT systems, networks, and data, or establish compensating controls when constraints or limitations of the University prohibit a complete separation of duties. The ISO Standard requires the University to segregate conflicting duties and conflicting areas of responsibility. By allowing the same individual that performs data removal to verify data removal, the University increases the risk of fraud, error, and bypassing of information security controls (University Standard, section 8.2 Access Determination and Control; ISO Standard, section: 5.3 Segregation of duties).

- The University did not complete a Surplus Form, PU19, to initiate its IT surplus and disposal process for all 25 assets sampled. The University's Surplus Procedures requires departments to complete the PU19 form to initiate the IT asset surplus and disposal process and indicate the equipment is ready for the IT department to pick up. Without completing the PU19 form for each IT asset the University processes through the surplus or disposal process, the University cannot ensure that it retains proper documentation for future reconciliation (*Surplus Procedures, step 1; ISO Standard, section: 7.10 Storage Media*).

- For three out of 25 sampled assets (12%), the University did not document in the change ticket the surplus and disposal process staff used for the three IT assets. The University's Surplus Procedures requires staff to create a change ticket for each batch of IT assets going through the surplus and disposal process and to indicate whether staff sanitized or destroyed the IT asset. The University Standard and ISO Standard requires the University to sanitize digital media prior to disposal. Without documenting whether staff sanitized or destroyed the IT asset within the change ticket, the University cannot validate that its staff properly removes sensitive data during the IT asset surplus or disposal process (*Surplus Procedures, step 9; University Standard, section: 10.2.2 IT Asset Management; ISO Standard, section: 7.10 Storage Media*).

- The University did not document its verification of data removal for 19 out of 25 sampled assets. The University's Surplus Procedures require the Technology Assistance Center (TAC) Manager to notate their verification in the change ticket that staff appropriately erased and tested the machine that is ready for disposal. The University Standard also requires staff to sanitize digital media prior to disposal. Without documenting the verification of data removal, the University cannot ensure its staff properly sanitizes its confidential and mission essential data from its IT assets (*Surplus Procedures, step 9; University Standard, section: 10.2.2 IT Asset Management*).

- The University does not define and document all elements of its procedures for destroying IT assets and the minimum and maximum time requirements for when staff should wipe, sanitize, and/or destroy IT assets. The ISO Standard requires the University to define, approve, communicate to relevant personnel, and review topic specific policies to further mandate the information of information security controls. Additionally, the ISO Standard requires the University to manage storage media throughout its life cycle of acquisition, use, transportation, and disposal, and when accumulating storage media for disposal, the University should give consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive. The University verbally sets a minimum two-week requirement for storing surplus equipment and a maximum 90-day goal for wiping, sanitizing, and/or destroying surplus equipment. However, without formally defining a process for destroying all storage media, the University increases the risk that staff will not properly and consistently destroy and dispose of its storage media, which could compromise the confidentiality of the University's mission essential and sensitive data. Also, without formally defining the University's expected time periods concerning the storage, wiping, and disposal of media, the University increases the risk of inconsistent practices, which could result in unauthorized disclosure, modification, removal, or destruction of sensitive information on storage media (*ISO Standard, sections: 5.1 Policies for information security, 7.10 Storage Media*).

The University's lack of defining requirements and expectations in formal policies and procedures and enforcing all aspects of its process and requirements led to its staff not consistently performing certain tasks as described above. The University should review and revise its policies and procedures to define and document all elements and expectations of its IT asset surplus and disposal process. The University should also implement an oversight process to ensure that staff are consistently following its IT asset surplus and disposal process throughout the lifecycle of each IT asset. This will assist the University in protecting the confidentiality of its sensitive and mission critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 5, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Radford University

Bret Danilowicz
President, Radford 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 discretely presented component unit of **Radford 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 June 5, 2024. Our report includes a reference to another auditor who audited the financial statements of the component unit of the University, as described in our report on the University's financial statements. The other auditor did not audit the financial statements of the component unit 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 the component unit of the University.

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 opinions 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 deficiencies in internal control titled "Dedicate Additional Resources to Financial Reporting," "Improve Timeliness of Bank Reconciliations," "Improve IT Risk Management and Contingency Planning Documentation," and "Improve IT Asset Management," 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 Risk Management and Contingency Planning Documentation" and "Improve IT Asset Management."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 4, 2024. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the finding 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

We did not perform audit work related to the findings included in our report dated June 6, 2022, titled "Improve Compliance over Enrollment Reporting" and "Promptly Return Unclaimed Aid to the Department of Education," because the University did not implement corrective action during our audit

period. We will follow up on these finding during the fiscal year 2024 audit. The University has not taken adequate corrective action with respect to the other prior audit finding identified as ongoing 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

ZLB/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Dedicate Additional Resources to Financial Reporting	Ongoing	2022
Improve Timeliness of Bank Reconciliations	Ongoing	2023
Improve IT Risk Management and Contingency Planning Documentation	Ongoing	2023
Improve IT Asset Management	Ongoing	2023
Improve Compliance over Enrollment Reporting	Ongoing**	2018
Promptly Return Unclaimed Aid to the Department of Education	Ongoing**	2021

* A status of **Complete** indicates adequate corrective action taken by management. **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

** These prior audit findings were not included in the scope of our audit. Per inquiry with management, we determined that corrective action was ongoing as of June 30, 2023.

June 21, 2024

The Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations for the year ended June 30, 2023 that were discussed during the financial statement audit exit conference.

Radford University acknowledges and concurs with the audit findings. The following contains management's response to each finding.

Dedicate Additional Resources to Financial Reporting

As noted, the University has made great strides complying with the increasing complexity and burden of the new accounting standards. The issues as reported in FY22 were not repeated in nature, the newly implemented flux and analysis procedures worked as intended, and changes to net position from the original unaudited financials were immaterial to net position. The University has continued to refine procedures, add review checks and balances, and implement solutions to address issues.

Specifically, the following actions have been completed or are planned:

1. The Department of General Accounting created a new position, the Assistant Manager of General Accounting, to provide increased capacity, allow for cross training with the Manager of General Accounting and Financial Reporting duties, and provide for resilience in turnover.
2. The former Manager of General Accounting rejoined the University as the full-time reconciliation accountant, supporting opportunities for institutional knowledge to be re-introduced and to provide cross training opportunities.
3. The University began searching for comprehensive software solutions to help automate manual procedures and provide quality review and analysis opportunities. This is expected to help specifically in addressing footnote issues and preparing for reporting model changes for FY26. The software solution is expected to be implemented in FY25.
4. The University is creating a new position in FY25, Financial Reporting Accountant, to provide increased capacity focused on financial reporting areas and new standards effective in FY25 and FY26.

Improve Timeliness of Bank Reconciliations

Radford University agrees that the June 2023 bank reconciliation was not completed timely. This issue was detected, addressed, and resolved by the University as fast and responsibly as it could have been.

The decision to use the May 2023 General Fund cash balance was based on the most accurate and available information at the time. The University, going forward, will document the acceptable tolerance level, based upon the statement balance for items not related to timing differences, in the reconciliation procedures and include the escalation process for amounts exceeding the threshold. The reconciliation procedures will be updated by June 30, 2024.

Since this issue occurred, corrective actions have been implemented. The bank reconciliation procedures have been revised so that they are replicable in the event of future turnover. After new procedures were put in place in December 2023 the monthly bank reconciliations have been completed and reviewed timely. Any further exceptions shall be addressed immediately for further refinement of the procedures as needed.

Radford University is committed to the timely preparation and review of bank reconciliations and following the CAPP Manual.

Improve IT Risk Management and Contingency Planning Documentation

- Although the Information Technology Services (ITS) teams have participated in tabletop exercises, the University acknowledges that it has not fully tested its Disaster Recovery Strategy. In FY22, ITS began a plan to use AWS Elastic Disaster Recovery as a mechanism to back up and test system recoveries, and ITS expects to complete that implementation and conduct and document system recovery testing by November 15, 2024. Also, by November 15, 2024, ITS will establish a regular schedule for testing the Disaster Recovery Strategy at least annually or whenever there are significant changes to the IT environment.

- As noted, there were seven systems that were classified as sensitive, but did not specify which of the three attributes (confidentiality, integrity, or availability (CIA)) was rated as high. The security controls implemented for these systems were appropriate and consistent with the sensitivity level of the systems; however, going forward, the Chief Information Security Officer will ensure that the CIA ratings are more closely reviewed and updated in ServiceNow to support the classification of each sensitive system.

- The University acknowledges that the revision history of the University Standard was not updated to reflect that a review was performed in 2023 even though no changes were necessary. Going forward, ITS will update the revision history of the document annually to provide evidence of compliance with the review cycle, regardless of whether any changes are made.

Improve IT Asset Management

- The University has established desktop procedures that ensure a separation of duties for data removal and verification for most IT assets, such as laptops and desktops. The procedures require that the staff who perform the sanitization are different from the staff who verify the completion of the process and sign off on the Surplus form. However, for some server hard drives, due to the specialized technical skills required and limited staff available, the same individual may perform both the data removal and verification steps. For instances in which this may occur, the University has implemented compensating controls that mitigate the risk of data breach or leakage for the server hard drives. Those compensating controls include a rigorous multi-step process to ensure that the data is irretrievable; the steps include physical removal of the hard drives from the servers,

configuration of the hard drives in a RAID array, wiping of the hard drives with a tool that overwrites the data with zeros, and physical destruction of the hard drives by drilling holes in them.

- As discussed, the Surplus Form, PU19, is not the only method that is used to collect and dispose of IT assets. Computer distribution workshops and one-on-one sessions where employees return their old computers as they receive new ones are also methods that are used; with those methods, no PU19 form is required. Regardless of the method used, the same sanitization procedures are followed. ITS will coordinate a review of the Surplus Property Policy and Procedures with the policy's oversight department to determine whether clarifications are needed regarding the PU19 form and, if so, update it accordingly. The review and update, if needed, will be completed by January 15, 2025.

- The University acknowledges that the technician neglected to document in the ticket the sanitization process utilized for the three identified IT assets. ITS will reinforce the appropriate procedures with all ITS personnel responsible for surplus and disposal.

- The University acknowledges that the employee neglected to document in the ticket the verification process for the nineteen identified assets. ITS will reinforce the appropriate procedures for documenting the verification step.

- The University acknowledges that the procedures for destroying IT assets do not specify the minimum and maximum time requirements for when staff should wipe, sanitize, and/or destroy IT assets. However, the University has implemented adequate compensating controls to ensure the security of the equipment and data until they are sanitized. Surplus property and data destruction are important, but not urgent, tasks; due to limited staffing resources, defining a specific time frame for completing these tasks could prevent Technology Support (Help Desk) staff from doing more critical support tasks, such as providing user assistance, troubleshooting issues, and installing software. Although the IT assets are securely stored until data destruction, effectively mitigating the risk, ITS will work towards implementing a maximum 90-day process for destroying IT assets and will document this in the procedures by November 1, 2024.

We would like to thank you and your staff for the valuable services that you provide.

Sincerely,

Robert Hoover, Ed.D.
Vice President for Finance & Administration and Chief Financial Officer