UNIVERSITY OF VIRGINIA
BOARD OF VISITORS

Meeting of the Audit, Compliance, and Risk Committee

March 1, 2024

AUDIT, COMPLIANCE, AND RISK COMMITTEE

Friday, March 1, 2024
9:45 a.m. – 11:15 a.m.
Board Room, The Rotunda

Committee Members:

Thomas A. DePasquale, Chair
Rachel W. Sheridan, Vice Chair
Mark T. Bowles
Carlos M. Brown
The Honorable Paul C. Harris
Babur B. Lateef, M.D.

Stephen P. Long, M.D.
The Honorable L.F. Payne
Amanda L. Pillion
Douglas D. Wetmore
Robert D. Hardie, Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

III.   **CLOSED SESSION**
- Discussion of information technology systems cybersecurity risks and cybersecurity enhancement plans where discussion in an open meeting would jeopardize the security of UVA Academic Division information technology systems and networks.
- Consultation with UVA Counsel on legal issues related to financial reporting.
- Discussion of proprietary, business-related information about the operations of the Medical Center, the School of Medicine, and the School of Nursing, where disclosure at this time would adversely affect the competitive position of the Medical Center, the School of Medicine, or the School of Nursing, specifically:
  - Strategic financial considerations and efforts in light of market and regulatory changes for the Health System and expected impact for FY2024, which further the strategic initiatives of the Medical Center and include proprietary metrics.
- The relevant exemptions to the Virginia Freedom of Information Act authorizing the discussions and consultations described above are provided for in Section 2.2-3711(A)(8) and (22), and Section 2.2-3705 (14 (b)) of the Code of Virginia.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: March 1, 2024

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Mr. Thomas DePasquale, the Committee Chair, will open the meeting and provide an overview of the agenda.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: March 1, 2024

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II. Audit Department Status Report

ACTION REQUIRED: None

BACKGROUND: To facilitate the Committee's oversight of internal controls, risk management, and compliance, the written report summarizes UVA Audit's work performed during the period **November 16, 2023- January 31, 2024**:

1) Executive summary of audit activities for the period
2) New findings for reports issued since the December 2023 Audit, Compliance, and Risk Committee report
3) Progress on BOV approved audit plan for FY2024

Executive Summary of Audit Activities for the Period
5 audits and investigations completed
Audit Department Support for University Committees and Initiatives: • Member of Policy Review Committee (Academic Division) • Member of Administrative Operations Artificial Intelligence Steering Committee (EVP COO Initiative) • Member of Enterprise Risk Management Network (Academic Division) • Member of IT Security Advisory Committee (Pan-University)

Looking Forward	Risks to Audit Plan Completion
The Institute of Internal Auditors (The IIA) has updated the profession's Global Audit Standards. UVA Audit will evaluate the impact the new standards will have on our charter and processes. The Committee will be updated in June. A refreshed 2-year risk-based internal audit plan will be reviewed with and approved by the Committee at the June meeting.	• Achievement of the approved UVA Health audit plan for FY2024 is at risk due to delays caused by internal audit staffing resource availability and delayed responses to audit information requests on audits in progress. • Completion of Academic Division IT audits for FY2024 are also at risk due to management's request to delay audits due to competing priorities (new initiatives, response to prior security incidents).

New findings in reports issued since December 2023 Audit, Compliance, and Risk Committee report	
Audit	**Summary of Report and Findings**
UVA Health Ransomware Assessment (IT Audit) `4` `3` 4 Partially Meets IT control-related findings. 3 controls met the control objectives.	In October 2021, Mandiant performed a Purple Team Assessment at UVA Health (UVAH) to evaluate Incident Response capabilities and procedures. Mandiant observed how UVAH's incident response mechanisms and protocols performed, offering an analysis of their effectiveness. Mandiant's report, issued in March 2022, was leveraged by the internal audit team in collaboration with management to determine if the recommendations were appropriately addressed and closed by management. Of the seven (7) Mandiant recommendations assessed, we observed three (3) action plans to address them met the control objective, and four (4) partially met the control objective. After receiving the draft report, management implemented corrective action plans for two of the recommendations found to be partially met during testing.
Child Development Centers `1` `1` `1` `2` 1 Priority 1, 1 Priority 2, 1 Process Improvement, 2 working controls	We assessed the oversight controls for contracted child day care services that ensure regulatory compliance and promote safety and security for the three centers that service UVA Academic Division and UVA Health employees. Our assessment indicated that operating controls for oversight are functioning effectively and address relevant risks, except for one Priority 1 observation involving building safety and security and one Priority 2 observation involving oversight processes for the three Child Development Centers we reviewed.
Community Health `2` `2` 2 Priority 1 Findings 2 Process Improvements	Project was conducted under Attorney-Client Privilege. Management is working to address the identified issues.

Status of Management's Action Plans to Remediate Control Deficiencies

The Institute of Internal Auditor's *Standard 2500: Monitoring Progress* requires the chief audit executive to establish and maintain a system to monitor the disposition of results communicated to management. The table below shows the number of action plans to correct control deficiencies that have not been implemented by the due dates *established by management*. (Reflects status as of January 31, 2024 for action plans due by 12/31/2023.)

All Open Corrective Action Plans

79%   50 Open Not Yet Due   63 All Open Action   17 Extended   27%

13 Open Past Due   21%
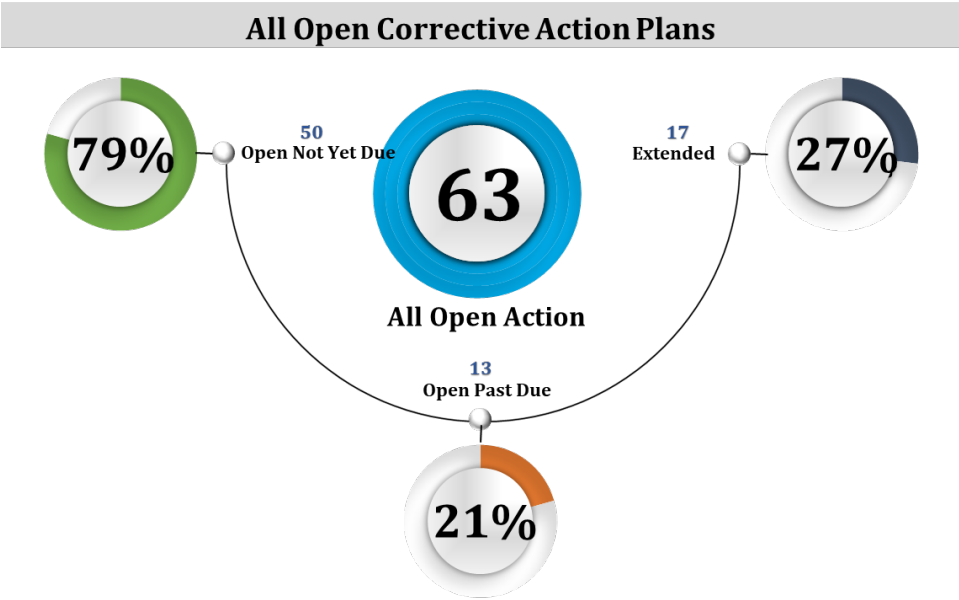
Notes: Eleven (11) action plan due dates were extended before they were overdue. Six (6) action plans were extended once the due date for completion had passed. Total extended plans: 17.

Average duration of open action plans: 341days (calculated from close of audit to January 31, 2024).

Audit	Action Item	Priority Rating	Action Plan Owner
2019 Fixed Fee Monitoring and Management	Two action items from this audit remain outstanding. These actions include the implementation of a residual balances policy and the associated monitoring metrics. As of February 2024, a draft policy has been submitted to the University's Policy Review Committee for approval. **Originally due: 6/30/2020** **Extended to 1/14/2022**	2 Priority 2 (P2) control gaps	Stewart Craig, Executive Director, Office of Sponsored Programs
2020 Accounts Payable	Two action items from this audit remain outstanding: 1) monitoring for potential employee/vendor conflicts of	2 Priority 2 (P2)	Mark Cartwright, Senior Director of Procurement

| Audit	Action Item	Priority Rating	Action Plan Owner
	interest, and 2) post transaction monitoring in Workday. PSDS will begin monitoring for 1 and 2 quarterly, beginning March 31, 2024. As a complementary control, PSDS is also enhancing the supplier onboarding process to provide additional screening for COI. **Originally due: 6/30/2022.First extended to 10/31/2022. Second extension granted to 11/30/2023**	control gaps	& Supplier Diversity Services (original Action Plan Owners were predecessors in equivalent position)
2021 Research Conflict of Interest *	One action plan from this audit remains outstanding; updating policy PROV-009, which as of February 2024, is circulating for approval. **Originally due: 12/31/2021**	1 Priority 2 (P2) control gap	Margaret Harden, Associate Provost for Academic Administration
2021 – DISM Computer Science – SEAS	One action item from this audit remains past due. This issue concerns network monitoring (e.g., non-compliance of policy required vulnerability scans and installation of anti-malware on network-connected devices). **Originally due: 6/30/2021** • First extended 5 months to 11/10/2021 • Second extension: granted an additional 7 months to 5/31/2022 • Third extension: granted an additional 20 months to 1/31/24 • **Fourth extension: granted an additional 2 months to 3/31/2024**	1 Partially Meets Policy (ISO 27002) control gap	Paul Henderson, Computer Systems Senior Engineer – SEAS
2022 Safety & Security Program Assessment - Follow Up	Three action items from this audit are past due. 1) The consolidation of the Medical Center workplace violence coordinator position into the Department of Safety and Security Division of Threat Assessment. Current plan: An assessment of University and Medical Center committees that	3 Priority 2 (P2) control gaps	Timothy Longo, Associate Vice President for Safety and Security / Chief of Police

Audit	Action Item	Priority Rating	Action Plan Owner
	support threat assessments, workplace violence, etc. will be completed, resulting in a gap analysis and definition of role and scope of the Workplace Violence coordinator position and an MOU between the EVP/COO and MC leadership. As of February 2024, discussions are still underway, and MC staff are developing a job description and organizational structure for the position. 2) The consolidation of the Fire Safety Program under the AVP for Safety and Security. 3) The housing of all safety and security functions in a dedicated command center. Current plan for #2 and #3: Organizational discussions have been initiated concerning the consolidation of the Fire Safety Program and space planning for the dedicated command center. As of February 2024, engineering work has commenced on the Zehmer Hall renovations and construction is scheduled to begin in August of 2024. **Originally due: 6/30/2023** **Extended to 3/31/2024**		
2023 Workday Financial Controls: Expense Reimbursements	One action plan is past due. The action plan stated that a process would be implemented to ensure ongoing review and notification of incomplete and aging account certifications in Workday. In January 2024, management constituted a workgroup to enhance the account certification process. Management anticipates process enhancement recommendations from the workgroup by May 2024 and project roll out by August 2024. **Originally due: 8/31/2023**	2 Priority 2 (P2) control gap	Jacob Mair, Senior Director of Accounting and Financial Reporting UVA Finance; Clara Tang, Senior Compliance Analyst UVA Finance
2023 School-Level Audits:	One action plan is past due. As of February 2024, McIntire has adopted	1 Priority	Pierce Coughter, Director of

Audit	Action Item	Priority Rating	Action Plan Owner
Pilot Audit of McIntire School	an alternate payment mechanism that eliminates the need to use gift cards; management expects the existing inventory of gift cards to be depleted by March 31, 2024. **Originally due: 11/30/2023**	2 (P2) control gap	Undergraduate Admissions and Marketing, McIntire
2023 Hazardous Materials Handling: Heating Plant Coal Lifecycle	One action plan is past due. The action plan related to arranging a tour of the Heat Plant for the UPD Patrol Officers. Management now expects this to occur by April 1, 2024. **Originally due: 12/31/2023**	1 Priority 2 (P2) control gap	Paul Zmick, Director of Energy & Utilities, Facilities Management, & Carey Drayton, Director, Safety & Security Systems & Technology
HIPAA Security Risk Assessment Follow-up	One action plan is past due. The action plan related to strengthening password standards. **Originally due: 8/31/2023** **Extended to: 12/30/2023**	1 Does Not Meet (DNM) Issue	Phil Napier, Information Security Officer, UVA Health

*Audit performed under engagement of University Counsel

BOV Approved Audit Plan Progress (Year to Date)

Because the plan is intentionally dynamic to maintain its relevance, a status report on the department's activities is provided at each Committee meeting.
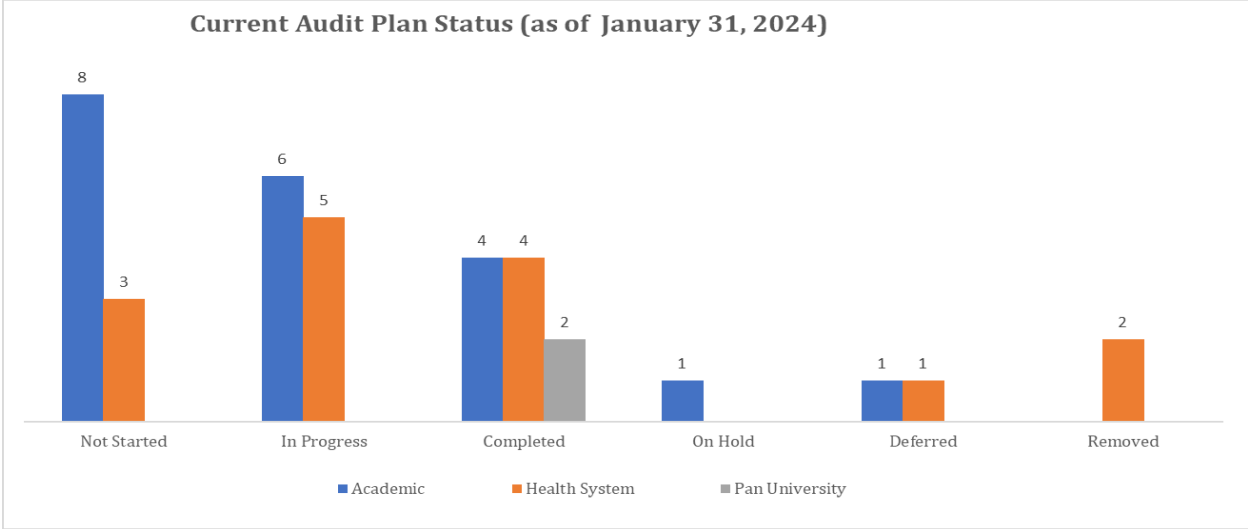
	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
1	Academic & UVA Health	Child Development Centers	Identify and assess oversight controls for contracted child day care services that ensure regulatory compliance and promote safety and security.	**Completed** (Replaced School-Level Audit 3)
2	Academic & UVA Health	ESG - Sustainability Reporting	Assess controls ensuring relevant, quality information is captured through the reporting process, culminating in the preparation of reliable sustainability reports.	**Completed**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
1	Academic	CARES Compliance - Higher Education Emergency Relief Fund (HEERF I, II, III) - Part 3 (FY24)	Evaluate design and effectiveness of controls and processes related to HEERF funds data collection, use, accounting, and reporting.	**Completed**
2	Academic	Construction Projects:	Using an outside expert in construction project management accounting, perform procedures relevant to phases of specified construction projects.	
		Football Operations Building Construction Audit		**Phase 1 Risk Assessment Completed**
		Hotel and Conference Center Construction Audit		**On Hold**
3	Academic	IT Disaster Recovery – Academic (IT Audit)	Determine and evaluate if adequate processes are in place for recovering critical systems and data in the event a service disruption or breach occurs.	**Not Started**
4	Academic	NCAA Compliance: Financial Aid for Student-Athletes	Assess UVA Athletic Department Compliance Office's oversight of student- athletes Financial Aid considering anticipated impacts of the NCAA Name, Image, and Likeness (NIL) policy.	**Not Started**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
5	Academic	Payroll Processing Review	Evaluate controls over payroll processes including Workday user access, identification of employees working out-of-state/country, and untimely terminations resulting in overpayments.	**In Progress**
6	Academic	Presidential Travel and Expense	Annual audit of the President's Travel and Entertainment expenses. Audits were paused during pandemic-impacted years. Audit will cover FY23 expenses.	**Completed**
7	Academic	Ransomware Assessment Follow Up – Academic (IT Audit)	Determine if the recommendations outlined within the December 2021 Mandiant Purple Team Report for the Academic Division have been addressed and closed by Management.	**Not Started**
8	Academic	Residential Colleges	Compare processes and analyze data related to governance, budgeting, spending, funding, and financial oversight for each of the three residential colleges (Brown, Hereford, and the International Residential College)	**In Progress** (Added to the Plan)

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
9	Academic	School-Level Audits: Pilot Audit of McIntire School	Complete pilot of school level audit program as a prelude to annual school level audits.	**Completed**
10	Academic	School-Level Audits (1) - UVA Engineering	Assess effectiveness of risk-relevant school level controls and processes at 3 UVA schools.	**In Progress**
11	Academic	School-Level Audits (2) - TBD	Annual school level audit	**Not Started**
12	Academic	Student Financial Services	Evaluate design and effectiveness of controls over accuracy and timeliness of student billing and accounts receivable.	**In Progress**
13	Academic	Third Party Risk Management – Academic (IT Audit)	Identify and assess the controls supporting the third-party risk management program such as: governance & operating model, policies, and procedures, third party data management, risk models, assessment methodology, and tools and technology used to support reporting.	**Not Started**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
14	Academic	Threat & Vulnerability Management – Academic (IT Audit)	Evaluate UVA Academic Systems controls supporting the Threat & Vulnerability Management program used for identifying, classifying, prioritizing, remediating, and mitigating software, and firmware vulnerabilities.	**Completed**
15	Academic	UVA Wise Academic Records - Degree Related Data (Jenzabar)	Evaluate design and effectiveness of controls over the maintenance of degree- related data, including grade submissions and changes, course substitutions and/or degree requirement exceptions, and incoming transcripts.	**Not Started**
16	Academic	Workday Benefits Administration	Follow-up on KPMG recommendations for the UVA Health Plan.	**Deferred**
17	Academic	Workday Financials Controls Validation: Gifts	Assess the effectiveness of key financial business process controls related to the acceptance, receipt, recording, and processing of gifts to the University.	**Not Started**
18	Academic	Workday Financials Controls Validation: Grants and Contracts	Assess the effectiveness of key financial business process controls related to expenditures of sponsored funding.	**In Progress**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
1	Health System	Contract Management	Internal controls over contract development, approval, and management. (Deferred to FY2025)	**Deferred**
2	Health System	Exclusion Screening for Vendors	Policies and procedures designed to ensure all on-site vendor representatives receive the required screening for potential exclusion from government payer programs. (Deferred to FY2025)	**Deferred**
3	Health System	PeopleSoft ITGC (IT Audit) - Health	Identify the methods, processes, and controls by which access is provisioned and deprovisioned both centrally and for selected applications that authorize access to end users.	**In Progress** (Replaced Identity & Access Management IT Audit)
4	Health System	Incentive Compensation Plans – University Hospital	Internal controls around the University Hospital's incentive compensation plans.	**In Progress**
5	Health System	Laboratory Outreach Billing (Non-patient receivables)	Billing and collection processes for the laboratory's outreach program (services provided to other organizations).	**In Progress**
6	Health System	Medical Device Recalls and Credits	Policies and procedures for claims adjustments related to medical device recalls.	**Removed**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
7	Health System	PeopleSoft Segregation of Duties Analysis (Attorney Client Privileged)	Attorney-Client Privileged	**In Progress** (Added to the Plan)
8	Health System	Pharmacy 340B Program – UVA Community Health	Compliance to Pharmacy 340B regulatory requirements and assess practices for maximizing realized savings.	**In Progress**
9	Health System	Attorney-Client Privileged	Attorney-Client Privileged - Deferred from FY2023	**Completed**
10	Health System	Provider Based Billing Compliance	Assess compliance with Medicare's billing rules for provider-based clinics.	**Removed**
11	Health System	Ransomware Assessment Follow Up (IT Audit)-Health System	Determine if the recommendations outlined within the December 2021 Mandiant Purple Team Report for the Health System have been addressed and closed by Management.	**Completed**

	Division	Audit Plan Topic	Scope	Status as of January 31, 2024
12	Health System	Third Party Risk Management (IT Audit)	Identify and assess the controls supporting the third-party risk management program such as: governance & operating model, policies, and procedures, third party data management, risk models, assessment methodology, and tools and technology used to support reporting.	**Completed**
13	Health System	Timely Encounter Closure – Professional Services	Level of compliance with Revenue Cycle standards for timely charge entry to patient accounts.	**Not Started**
14	Health System	Trauma Activation Claims – Billing Compliance	Validate that Medicare claims for trauma services comply with Medicare billing guidelines.	**Completed**
15	Health System	UVACH: IRS 501(r) Compliance	Compliance with IRS 501(r) rules applicable to non-profit hospitals, such as community needs analyses and community benefit plans, financial assistance elements and publication. (Deferred from FY2023)	**In Progress**
16	Health System	Warehouse Receiving Controls	The receiving processes at the new distribution warehouse – internal control design and effectiveness.	**Not Started**

3. Summary of Audit Findings Year to Date (July 1, 2023 through January 31, 2024)

The table below summarizes audit findings by priority rating for audits performed in FY2024.

Audit Name	Division	Priority-Rating					
		P1	DNM	P2	PM	OP	W
CARES Compliance - Higher Education Emergency Relief Funds	Academic					1	4
Threat and Vulnerability Management	Academic		1		3		9
McIntire School of Commerce	Academic	1		4		3	16
Contract Labor Controls	UVA Health	2		3			2
Trauma Activation	UVA Health	No audit findings					
Third-Party Risk Management	UVA Health		2		9		4
Ransomware Assessment Follow-up	UVA Health				4		3
Community Health**	UVA Health	2				2	
Salesforce Service and Marketing Cloud (IT Audit)	Pan-University						10
ESG - Sustainability Reporting	Pan-University			1		1	2
Presidential Travel and Expense	Pan-University					1	3
Child Development Centers	Pan-University	1		1		1	2
Total Rated Findings Fiscal Year to Date		6	3	9	16	9	55

**Project conducted under Attorney-Client Privilege

	Rating Scale		
P1	**Priority 1**	A Priority 1 item signifies a control and/or process deficiency of sufficiently high risk that it provides minimal or no assurance that institutional objectives will be achieved. Management must take immediate corrective action to mitigate Priority 1 deficiencies.
DNM	**Does Not Meet**	An IT control that is not in place or is ineffective to achieve the relevant IT controls framework (e.g., ISO-27002-2013) requirement
P2	**Priority 2**	A Priority 2 item signifies a control and/or process deficiency that hinders the effectiveness and efficiency of unit level operations, potentially impeding the attainment of institutional objectives. Management must take timely corrective action to mitigate Priority 2 deficiencies.
PM	**Partially Meets**	An IT control that meets some, but not all, of the relevant IT controls framework (e.g., ISO-27002-2013) requirement
OP	**Process Improvement**	A process improvement item signifies an opportunity to achieve additional control and/or process efficiencies.
W	**Working**	Control tested or process evaluated is working as designed

UNIVERSITY OF VIRGINIA

BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: March 1, 2024

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. Records and Information Management Report: Board of Visitors Records Retention Guidance

ACTION REQUIRED: None

BACKGROUND: During the September 14, 2023 board meeting Ms. Caroline Walters, University Records Officer, provided an overview of Records and Information Management and shared information of which board members should be aware. During that presentation, Ms. Walters was asked to prepare a short summary of information about records retention that board members may reference and to be added to the orientation of new board members to manage their records in compliance with the Virginia Public Records Act. The Board of Visitors Records Retention Guidance document can be found in the attachment.

ATTACHMENT

Board of Visitors Records Retention Guidance
February 6, 2024

Virginia Records Laws:
- **Virginia Public Records Act:**
  https://law.lis.virginia.gov/vacodepopularnames/virginia-public-records-act/. The VPRA specifies records created should not be destroyed until the retention time has expired and all issues (FOIA, litigation, audit & investigation) have been closed. Permission to destroy official records is granted by the University Records Officer.
- **Virginia Freedom of Information Act:**
  https://law.lis.virginia.gov/vacodepopularnames/virginia-freedom-of-information-act/ specifies that the people of the Commonwealth have ready access to public records in the custody of public bodies or its officers and employees. Officer and Employees must turn over records requested, regardless of form or storage medium.

What is a record?
Recorded information that *documents a transaction or activity by or with any appointed board member*, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information *is a University record if it is produced, collected, received, or retained in pursuance of law or in connection with the transaction of University business.* The *medium upon which such information is recorded has no bearing* on the determination of whether the recording is a University record.
(IRM-017 Records Management https://uvapolicy.virginia.edu/policy/IRM-017)

- **Official Records** are maintained by the creator or the person who receives information from outside of the University.
- **Reference Copies** may be destroyed when reference value ends. The official records are maintained by the official recordkeeper – for example: The BOV Office maintains the official record of all BOV meeting minutes and attachments/presentations. Copies you have of these may be destroyed (paper or electronic) when you no longer need them.

What records am I responsible for as a member of the UVA Board of Visitors?
Correspondence/Communications – letters, memos, and any other communication, including those received and sent electronically. Emails, texts, messaging, and voicemail are considered correspondence, regardless of whether you use your university or personal accounts to conduct university business.
Reports/Meeting Minutes – information provided to board members for review or reference or to document the activities of the board, including committee work and related projects.

How long do I need to keep records?
Retention time varies depending on the content of the record. The full records retention schedule is available on the Records and Information Management (RIM) Website (https://recordsmanagement.virginia.edu/retention-schedules) Here are a few records series specific to the Board of Visitors.

- **101-100559 - Correspondence: Board of Visitors** Correspondence of the Board of Visitors members (non-Rector), including email. DOES NOT INCLUDE correspondence of the BOV Rector, Secretary, or BOV Office.
  Destroy 3 closed calendar years after termination of appointment.
- **101-100557 - Correspondence: BOV Rector** Correspondence of the Rector of the Board of Visitors. Includes all correspondence, including email.
  Transfer to University Archives after 10 years and when reference value ends.

Where is the best place to store records?
- **University Resources:** Highly recommended to store all University records within university provided resources, which may include Microsoft 365 (Email, OneDrive, Teams) and UVA Box.
- **Personal Devices:** Use personal devices sparingly, and never use a personal device to store official University records – including texts or other communications. When the university must respond to FOIA requests, litigation, and investigations, you may be required to provide access to your personal devices and accounts if you use them for University related communications. The RIM office can assist in transferring official records from your personal devices to UVA provided storage.
- **Professional Resources (non-UVA)**: Do not use resources provided by your paying job/career/business. Placing University records on these resources does not protect them from FOIA, litigation, or investigations and can create difficulty during discovery and collection of these matters.

*You may use a personal device or company device (non-UVA) to access UVA resources – such as logging into Box, OneDrive, or Email via a web browser.

Where can I get help with records questions:
The Records & Information Management Office is here to help. Feel free to contact us with questions. The RIM website features pre-recorded short training (5-10 min sessions) on topics including electronic records management, email management and RIM Basics.

Records & Information Management
Email: records@virginia.edu
Website: https://recordsmanagement.virginia.edu/