UNIVERSITY SYSTEM OF MARYLAND
BOARD OF REGENTS - AUDIT COMMITTEE
OPEN MEETING AGENDA

June 5, 2025

1.	Information & Discussion - Office of Legislative Audit Activity – Published Audit Reports	Mr. Mosca Mr. Sergi Mr. Lockett
2.	Information and Discussion – FY 2025 Audit Committee Objectives	Mr. Mosca
3.	Information – Update of HP Rawlings Examination	Ms. Bowman
4.	Information & Discussion – SB and Co, LLC – FYE 6/30/2025 Independent Audit Scope	Ms. Booker
5.	Information & Discussion – Update of USM Enterprise Risk Management	Mr. Eismeier Ms. Herbst
6.	Action, Information & Discussion – Recommended Modification of USM IT Security Standards – Version 5.1	Mr. Eismeier
7.	Information & Discussion – Review of Presidents, Chancellor, and Board of Regents CY 2024 Annual Financial Disclosure Compliance	Mr. Mosca
8.	Information & Discussion - Follow up of Action Items from Previous Meetings	Mr. Mosca
9.	Approval - Convene to Closed Session	Mr. Pope

Information & Discussion - Office of Legislative Audit Activity –

UNIVERSITY SYSTEM of MARYLAND

BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION, INFORMATION OR DISCUSSION

TOPIC: Update of Office of Legislative Audit Activity

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

University of Maryland Global Campus' Vice President and Chief Operating Officer and Vice President and Chief Financial Officer will provide an update on actions taken since its August 2024 audit report (Attachment A).

Since the Committee's March 2025 meeting, the Office of Legislative Audits (OLA) has issued its audit report on Bowie State University (Summarized in Attachment B).

Attachment C is a systemwide summary of audit findings in OLA's most recent reports for each institution.

OLA Engagements Currently Active:

- University of Maryland, Baltimore (Active since May 2024),
- University of Baltimore (Active since September 2024) and
- University of Maryland College Park (Active since January 2024),

Attachments

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: none

COMMITTEE ACTION: None DATE:

BOARD ACTION: None DATE:

SUBMITTED BY: David Mosca 6-5-2025

Date: June 5, 2025

To: USM Board of Regents Audit Committee

From: Gregory W. Fowler, Ph.D., UMGC President

Re: Update on OLA Audit Recommendations – August 2024 Report

Please find below the latest update on the implementation status of UMGC's responses to the recommendations outlined in the Office of Legislative Audits (OLA) report published in August 2024.

I am pleased to report that UMGC has addressed each recommendation within the specified timelines.

Should you have any questions or require further information, please do not hesitate to contact me.

UMGC OLA Audit Recommendations & Response Implementation Status

Finding 1

a. conduct periodic formal, documented, comprehensive evaluations, including a cost benefit analysis, to determine the extent to which the intended purpose, objectives, and goals of creating UMGC Ventures, AccelerEd, and HelioCampus, and placing AccelerEd and HelioCampus within Ventures have been achieved;

UMGC contracted with Attain Partners to conduct a formal comprehensive evaluation, including a cost benefit analysis, to determine the extent to which the intended purpose, objectives, and goals of creating UMGC Ventures and AccelerEd, and placing AccelerEd within Ventures have been achieved. The report was completed in May of 2025.

UMGC has also conducted a competitive best-value RFP to solicit Analytics services, which was awarded to HelioCampus.

b. review the aforementioned Ventures' activity to ensure that the related funds were used as intended;

UMGC has reviewed and collected source documentation for the activity related to bullets 2 and 3 of the auditors' analysis and determined that the funds were used as intended.

c. determine if any adjustment to its relationship with and continued use of these entities is warranted, for example whether any services should be brought back in-house; and

UMGC has chosen to reintegrate Ventures and AccelerEd back in to UMGC. The formal comprehensive evaluation conducted by Attain Partners recommended a 12–18-month reintegration period to allow time for UMGC to execute a plan to transition employees, services, and contracts into UMGC.

d. update the USM BOR on the results of the evaluations and any resulting adjustments.

UMGC will update the USM Chancellor and the BOR on the results of the evaluation performed by Attain Partners and the resulting adjustment UMGC has chosen at the June 13, 2025 BOR meeting.

Finding 2

a. take steps to ensure IT services are procured on a competitive basis;

UMGC has chosen to reintegrate Ventures and AccelerEd back in to UMGC. The study recommended a 12–18-month reintegration period to allow time for UMGC to execute a

plan to transition employees, services, and contracts into UMGC. Beginning 7/1/25, UMGC will ensure that all IT services are procured on a competitive basis.

b. adjust its Professional Services Agreement to require Ventures to provide documentation of the steps it takes to find the best qualified and most advantageous vendors for each SOW;

UMGC has adjusted its most recent Professional Services Agreement (7/1/24) to require Ventures to develop and utilize procurement procedures and policies that demonstrate and document a commitment to find the best qualified and most advantageous vendors for each SOW.

c. ensure that invoices include a breakdown of services provided and costs incurred for the period;

UMGC has adjusted its most recent Professional Services Agreement (7/1/24) to require Ventures to include a description of the services and costs incurred on invoices. UMGC staff review and reconcile the invoice and backup documentation monthly before approving payment.

d. discontinue the use of contingency fees without a clear definition of permitted usage, a requirement to report usage, and clarification as to the disposition of unused fees; and include the key components identified by the aforementioned vendor's report in future SOWs.

UMGC has discontinued the use of contingency fees in its most recent Professional Services Agreement (7/1/24) with Ventures.

Finding 3

a. ensure that contracted services are routinely, adequately, and independently monitored and evaluated to help ensure the proper and timely receipt of all required deliverables;

The UMGC Enterprise Project Management Office (EPMO) is routinely, adequately, and independently monitoring and evaluating large-scale IT projects, to ensure the proper and timely receipt of all required deliverables. The EPMO office has developed a framework for this monitoring and evaluation and reports out monthly.

b. ensure that a provision for liquidated damages for non-performance is included in its contracts; and

UMGC has adjusted its most recent Professional Services Agreement (7/1/24) with Ventures to reference applicable liquidated damages in SOW's.

c. consult with legal counsel regarding the potential for collecting liquidated damages relating to the closed SIS project noted in this finding.

UMGC has engaged its internal legal counsel as well as the State of Maryland Attorneys General Office to examine the potential for collecting liquidated damages related to the closed SIS project; the analysis was that it would be highly unlikely or impossible.

Finding 4

a. establish formal procedures for selecting and assigning work to prequalified vendors, such as the basis for selection and required documentation supporting the selection;

UMGC is documenting the basis for selection for prequalified vendors.

b. use competitive procurement within prequalified vendors for individual tasks;

As the auditors correctly point out, in reviewing the original RFP for Marketing Services dated January 18, 2018, there was language in Section 1.2 of the solicitation document issued stating that services were to be provided based on responses to Task Order Request for Proposals (TORP) solicited from the awarded master contractors. However, this language was inadvertently copied from a previous RFP for non-media services and there was never any intent to do secondary competition – and it had not been done during previous media contracts. Once this error was discovered during the procurement process, an addendum was issued by UMGC removing this error. UMGC sought and received approval from both the USM Board of Regents and the Maryland Board of Public Works outlining the not-to-exceed amounts of each awarded contractor for these services. The RFP process was rigorous and provided a process to ensure that UMGC selects the most capable and cost-effective vendor.

UMGC does agree to provide better documentation as requested in the audit as follows: establish formal procedures for selecting and assigning work to prequalified vendors, such as the basis for selection, required documentation supporting the selection, and employees authorized to make and approve the selection; ensure that task orders or SOWs contain sufficient details to enable effective monitoring and receipt of requested services and deliverables; and establish performance measures, such as impact on enrollment, when establishing SOWs to help direct future use of the contracts.
A secondary competitive procurement process with vendors who have already been selected through a competitive procurement process is impractical given UMGC's business model for advertising. UMGC follows a process of testing and learning to

establish and validate strong performance on multiple dimensions. The process of testing and learning, to establish strong performance provides sound diligence. Once a winning formula is achieved, it should not be disrupted lightly.

UMGC has made four vendor shifts over the past five years, but these decisions were made very carefully. As an example, one of these shifts reduced our CPM (cost-per-thousand impressions) on ConnectedTV from $34 to $14, a 59% savings. This shifting was endorsed by the Board of Public Works, who approved reallocation of spend authority across approved vendors on October 4, 2023, to allow proven vendors to spend more.

The significant headcount growth these past three years (new enrollments +9%, +12%, +12%) is in large part a result of this approach to advertising vendors. UMGC has been able to build tremendous momentum and outperform the education category.

The marketing team has continued to ensure the State of Maryland and UMGC receive the best value for its marketing investment and makes decisions on the technical merit and the acumen of each vendor.

c. ensure that task orders or SOWs contain sufficient details to enable effective monitoring and receipt of requested services and deliverables; and

UMGC is explicit in SOWs concerning the monitoring mechanisms that will ensure the receipt of requested services and deliverables.

d. establish performance measures, such as impact on enrollment, when establishing SOWs to help direct future use of the contracts.

UMGC explicitly states performance measures on SOWs which will help direct the future use of the contracts.

Finding 5

a. ensure that the sole source procurement method is used only when a single vendor can meet the contract requirements, and adequately document the sole source justification; and

UMGC conducted a competitive procurement for these services, and an award was made to the vendor that met the requirements.

b. consolidate sole source procurements for the same services and obtain required approvals when total procurement amounts exceed established limits.

UMGC conducted a competitive procurement for these two separate services. In the radio services procurement, no vendors met the minimum requirements, and a selection was not made, and the services were not contracted for. In regard to the digital advertising services, an award was made for a 3-year contract, the contracted amount did not require board approval.

Finding 6

a. record all checks received in the mail immediately upon receipt, and

UMGC has begun recording all checks received in the check log upon receipt.

b. ensure that deposit verifications are performed by an employee independent of the cash receipts functions using initial recordation documents.

UMGC has modified its deposit verification process to document the independent review verifying the amount deposited agrees with checks received.

Finding 7

We recommend that UMGC ensure that all residency status changes made are subject to independent review and approval by ensuring that all such changes are included on output reports currently used to conduct those reviews.

UMGC has begun to audit residency changes based upon effective date instead of the term.

Summary Analysis of Findings in OLA's Bowie State University Audit Report

The Office of Legislative Audits (OLA) issued its final report on BSU. OLA reports one fiscal compliance finding and two Cyber Security findings.

OLA's reported findings are summarized as follows:

Finding 1: Student Accounts Receivable

OLA reports that BSU did not ensure that adjustments to student accounts were proper and did not refer delinquent accounts to the State's Central Collection Unit (CCU) as required.

OLA also notes that BSU did not review $7.5 million in adjustments to students' accounts during the calendar year 2023. OLA did not identify any unsupported adjustments.

Finding 2: Cyber Security (Fully Redacted)

Finding 3: Cyber Security (Fully Redacted)

Information and Discussion – FY 2025 Audit Committee Objectives

UNIVERSITY SYSTEM of MARYLAND

BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION, INFORMATION OR DISCUSSION

TOPIC: Information & Discussion – FY 2025 Audit Committee Work Plan & Objectives

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

Attached is a schedule of the Audit Committee's (Committee) FY 2025 work plan and objectives. The objectives are designed to assist the Committee in fulfilling the requirements of its Charter and Bylaws. The schedule also identifies the objectives addressed at each Audit Committee meeting throughout the year.

On the whole, the Committee has met its objectives and fulfilled its requirements as defined in its Charter and Bylaws.

Attachment

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: none

COMMITTEE ACTION: None DATE:

BOARD ACTION: None DATE:

SUBMITTED BY: David Mosca

USM BOR Audit Committee
Annual Work Plan
FY 2025

Objective		When Performed Audit Committee Meetings						
		Oct	**Dec**	**Jan**	**Mar**	**June**	**As Needed**	**Completed**
Authority								
1	The Committee, with the approval of the Board, is empowered to retain outside counsel or persons having special competence as necessary to assist the Committee in fulfilling its responsibility.						x	N/A
2	Resolve any disagreements between the independent auditor and management.						x	N/A
Composition of Committee Members								
3	The Audit Committee shall comprise not less than **5** or more than **7** members. The majority of the members must be knowledgeable about financial matters.	x						Yes
Meetings								
4	Meet at least 4 times per year.	x	x	x	x	x		Yes
Responsibilities								
	Internal Audit							
5	Review with the Vice Chancellor for Accountability progress of completing the annual plan of activity.	x	x		x	x		Yes
6	Review and approve internal audit's annual plan of activity.		x					Yes
7	Ensure that there are no unjustified restrictions or limitations on the internal audit department.	x	x		x	x		Yes
8	Review the effectiveness of the internal audit function.					x		Yes
9	Meet separately with the Vice Chancellor for Accountability to discuss any matters that the committee or the VC believes should be discussed privately.	x	x		x	x		Yes
	Independent Auditor							
10	Review the external auditors' proposed audit scope and approach.					x		Yes
11	Review significant accounting and reporting issues and understand their impact on the financial statements.		x	x				Yes
12	Review with management and the external auditors the results of the audit, including any difficulties encountered.		x	x				Yes
13	Discuss the annual audited financial statements with management and the external auditors.		x	x				Yes
14	Review and discuss the results of enrolment testing agreed upon procedures.				x			Yes
15	Review and discuss the results of the Single Audit.				x			Yes
16	Discuss the scope of external auditors' review of internal control over financial reporting.		x					Yes
17	Review the performance of the external auditors, and exercise final approval on the appointment or discharge of the auditors.						x	N/A

USM BOR Audit Committee
Annual Work Plan
FY 2025

Objective		When Performed Audit Committee Meetings						
		Oct	**Dec**	**Jan**	**Mar**	**June**	**As Needed**	**Completed**
18	Meet separately with the external auditors to discuss any matters that the committee or auditors believe should be discussed privately.	x	x		x	x		Yes
	Financial Reporting							
19	Review FYE Consolidated Financial Statements	x	x	x				Yes
20	Review FYE Financial Dashboard Indicators		x					Yes
21	Review 12/31/24 six month Financial Statements				x			Yes
	Other							
22	Regularly report to the Board of Regents about Committee activities.	x	x	x	x	x		Yes
23	Confirm annually that all responsibilities outlined in the committee's charter have been carried out.					x		Yes
24	Discuss with the Attorney General or representative, the status of legal matters that may have a significant impact on USM institution's financial statements.	x	x		x	x		Yes
25	Review legislative audits of the institutions of the University System and institutional responses thereto, and provide the Board with appropriate reports.	x	x		x	x		Yes
26	Review policies pertaining to Audit Committee	x			x	x		Yes
27	Monitor the Board's observance of the State Ethics Code as it pertains to possible conflict of interest with matters of the University System of Maryland						x	N/A
28	Update Regarding ERM and Crisis Management		x			x		Yes
29	Receive updates of Cybersecurity environment and emerging risks.	x	x		x	x		Yes
30	Review Presidents, Chancellor and Board of Regents annual financial disclosure forms. This is to comply with Md. Education Code Ann. §12-104(p).					x		Yes
31	Review analysis of Office of Legislative Audit Findings	x			x	x		Yes

Information – Update of HP Rawlings Examination

TOPIC: Update – HP Rawlings Agreed Upon Procedures

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

SUMMARY:

Materials attached.

FISCAL IMPACT: Information item

CHANCELLOR'S RECOMMENDATION: Information item

COMMITTEE ACTION: DATE:

BOARD ACTION: DATE:

SUBMITTED BY: David Mosca

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

University System of Maryland

Audit Committee Meeting

June 5, 2025

Scope of Services and Deliverables- FY24 Status

Opinion on financial statements for the year ending June 30, 2024

- *Complete. Issued on 12/18/24*

Single audit testing as part of the State of Maryland Single Audit

- *Complete. Issued on 3/31/25*

Governance communication letter

- *Complete. Issued on 12/18/24*

Campus enrollment agreed-upon procedures

- *Complete. Issued on 11/5/24*

Howard P. Rawlings Scholarship Programs agreed-upon procedures

- *Complete. Issued on 6/1/25*

FY24 Single Audit Findings

Finding Number	Assistance Listing #	Repeat Finding	Federal Program	Institution	Internal Control		Compliance	Compliance Requirement
					Material Weakness	Significant Deficiency		
2024-020	84.031	2023-012	Higher Education Institutional Aid	BSU		X	X	Allowable Cost and Activities - Payroll: Time and effort was not documented and reviewed timely
2024-021	84.031	2023-013	Higher Education Institutional Aid	CSU		X	X	Allowable Cost and Activities - Payroll: Actual time and effort charged to the grant did not agree to the time and effort report.
2024-022	84.031	2023-015	Higher Education Institutional Aid	CSU, BSU, UMES		X		Suspension and Debarment was not verified with contractors prior to entering into transactions.

FY24 State Scholarship Testing

	Sample Size													
	EA	GA	CBEAG	Housing Status	CBEAG calculations	MDCAPS award amount	Drug Free Pledge	ISIR Mismatch	SAP	Zip Code	EFC	Enrollment Status	Federal Verification	Residency
Bowie State University	45	44	-	-	-	1	-	3	-	-	-	1	-	-
Coppin State University	44	7	1	6	1	2	-	-	1	1	-	-	-	-
Frostburg State University	44	9	2	-	-	-	-	-	-	-	-	-	-	-
Salisbury University	45	43	3	-	-	-	-	-	-	-	-	-	-	-
Towson University	46	45	38	-	-	-	-	-	-	-	-	-	-	-
University of Baltimore	43	1	1	-	-	-	-	-	1	6	1		-	-
University of Maryland, Baltimore	41	2	-	-	-	-	-	-	-	-	-	1	-	-
University of Maryland, Baltimore County	45	45	5	-	-	-	1	-	-	-	-	-	-	-
University of Maryland, College Park	45	45	4	5	-	5	-	-	2	1	-	1	8	1
University of Maryland, Eastern Shore	44	10	2	1	-	-	-	-	-	-	-	-	-	-
University of Maryland Global Campus	46	2	6	-	-	-	-	-	-	-	-	-	-	-

Information & Discussion – SB and Co, LLC – FYE 6/30/2025

TOPIC: SB and Co, LLC – FYE 6/30/2025 - Independent Auditor Planning

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

SUMMARY:

Materials attached.

FISCAL IMPACT: Information item

CHANCELLOR'S RECOMMENDATION: Information item

COMMITTEE ACTION: DATE:

BOARD ACTION: DATE:

SUBMITTED BY: David Mosca

Certified Public Accountants & Business Advisors

SBC

UNIVERSITY SYSTEM OF MARYLAND PLANNING MEETING WITH THE AUDIT COMMITTEE

University System of Maryland

Fiscal Year Ending June 30, 2025

June 5, 2025

Engagement Team Leadership

Gray Smith, CPA
Client Service Partner

- Over 40 years of public accounting experience
- Graduate of Hampton University
- Chief Executive Officer of the firm
- Former member of Federal Accounting Standards Advisory Board
- Former Arthur Andersen and Ernst & Young Partner
- Former Andersen College and University East Coast Lead

Monique Booker, CPA
Engagement Partner

- Over 30 years of public accounting experience
- Graduate of Hampton University
- Leads SBC's education sector
- Current member of AICPA's Executive Committee of Government Audit Quality Center
- Former member of AICPA's Auditing Standards Board
- Former Arthur Andersen Senior Manager

Stephen Mackall, CPA
Audit Partner

- Over 13 years of public accounting experience
- Graduate of Towson University
- Former Manager at KPMG, LLP

Richard Lee, CPA
Engagement Senior Manager

- Over 10 years of public accounting experience
- Graduate of Purdue University
- Former Senior Manager at KPMG, LLP

Audit Approach

- **Central Testing**
  - Cash & investments
  - Debt and worker's compensation
  - Appropriations
  - Net Pension liability
  - OPEB liability
- **3 Levels of Institution Testing (Rotation)**
  - Audit
  - Review
  - Analytical
- **Significant Risk Items at Institutions**
  - TBD
- **Federal Grant Compliance**
  - Rotation of single audit institutions

Level of Testing by Scope

Level	Understand Control Environment	Understand Effectiveness of the Design of Controls	Testing Effectiveness of Key Controls	Understand Financial Close Process	Financial Misstatement Analysis	Substantive Testing	Evaluate General IT Controls	Evaluate Applications IT Controls
Audit	X	X	X	X	X	X	X	X
Review	X	X		X	X	X *		
Analytical				X	X	X *		

* Certain substantive testing for high risk/problem areas

Scope and Location of Testing

	2025 Scope of Work				2024 Totals	
Institution	Audit	Review	Analytical	Single Audit	Assets	Operating Revenues and State Appropriations
Bowie State University		X			$ 551,299,937	$ 160,259,066
Coppin State University			X		364,880,373	93,949,449
Frostburg State University			X		339,485,808	112,655,351
Headquarters (cash, investments, debt)			X		692,120,139	27,893,219
Salisbury University		X			580,295,800	204,066,432
Towson University		X			1,577,025,240	479,004,154
University of Baltimore			X		283,495,430	128,430,416
University of Maryland Center for Environmental Science			X		108,846,497	57,031,523
University of Maryland Eastern Shore		X			328,611,711	150,047,199
University of Maryland Global Campus	X			X	570,512,753	406,501,927
University of Maryland, Baltimore	X			X	1,787,559,204	1,489,222,530
University of Maryland, Baltimore County	X			X	1,030,998,329	597,292,486
University of Maryland, College Park	X			X	3,971,318,339	2,575,061,536

	Audit		Review		Analytical		Total
Total Assets	$ 7,360,388,625	60%	$ 3,037,232,688	25%	$ 1,788,828,247 *	15%	$ 12,186,449,561
Total Operating Revenues and State Appropriations	5,068,078,479	78%	993,376,851	15%	419,959,958	6%	6,481,415,289

*Approximately $665 million of the total assets of analytical institutions represents 37% of total assets of the analytical institutions and will be substantively tested centrally

Engagement Timeline

Timing	Event
April	Planning meeting with System Headquarters
June	Audit Committee planning meeting
June/July	Preliminary fieldwork, including single audit walkthrough and first time audit procedures
July	Meet with management to discuss preliminary results
July/August	Single audit testing, enrollment testing and IT environment review
September/October	Final fieldwork
October/November	Exit conference with institutions regarding findings and recommendations
November	Meet with Audit Committee to review Financial Statement draft and observations
December	Audit Committee presentation on financial results
December/January	Complete single audit testing and findings
March	Audit Committee presentation on single audit results

Assessment of Control Environment

Area	Points to Consider
Control Environment	▪ Key executive integrity, ethics, and behavior ▪ Control consciousness and operating style ▪ Commitment to competence ▪ Exercise oversee responsibility ▪ Organizational structure, responsibility, and authority ▪ Enforce accountability ▪ HR policies and procedures
Risk Assessment	▪ Define objectives and risk tolerances ▪ Identify, analyze, and respond to risk ▪ Assess fraud risk ▪ Identify, analyze, and respond to change ▪ Mechanisms to anticipate, identify, and react to significant events ▪ Processes and procedures to identify changes in GAAP, business practices, and internal control
Control Activities	▪ Design control activities ▪ Design activities for the information system ▪ Implement control activities ▪ Existence of necessary policies and procedures ▪ Clear financial objectives with active monitoring ▪ Logical segregation of duties ▪ Periodic comparisons of book-to-actual and physical count-to-books ▪ Adequate safeguards of documents, records, and assets ▪ Assess controls in place

Assessment of Control Environment (cont.)

Area	Points to Consider
Information and Communication	▪ Use quality information ▪ Communicate internally ▪ Communicate externally ▪ Adequate performance reports produced from information systems ▪ Information systems are connected with business strategy ▪ Commitment of HR and finance to develop, test, and monitor IT systems and programs ▪ Business continuity and disaster plan for IT ▪ Established communication channels for employees to fulfill responsibilities ▪ Adequate communication across organization
Monitoring	▪ Perform monitoring activities ▪ Remediate deficiencies ▪ Periodic evaluations of internal controls ▪ Internal audit function ▪ Implementation of improvement recommendations

Evaluation of Key Processes

Process	Function
Treasury	▪ Cash Management ▪ Investment Accounting ▪ Investment Monitoring ▪ Investment Valuation ▪ Investment Policy ▪ Reconciliation ▪ Debt Accounting
Estimation	▪ Methodology ▪ Information ▪ Calculation
Financial Reporting	▪ Accounting Principles and Disclosure ▪ Component Unit and Affiliate Monitoring ▪ Closing the Books ▪ General Ledger and Journal Entry Processing ▪ Verification and Review of Results ▪ Report Preparation
Purchase Cards/Travel and Entertainment Reimbursement	▪ Card Issuance and Collection ▪ Training ▪ Purchase Accounting and Approval ▪ Monitoring ▪ Purchase Approval ▪ Travel and Entertainment Reimbursement

Evaluation of Key Processes (cont.)

Process	Function
Expenditures	▪ Purchasing ▪ Receiving ▪ General Ledger Coding ▪ Accounts Payable and Cash Disbursement
Payroll	▪ Hiring ▪ Attendance Reporting ▪ Payroll Accounting and Processing ▪ Payroll Disbursements ▪ Separation ▪ Contract Management
Revenue	▪ Billing ▪ Cash Receipts ▪ Revenue Recognition ▪ Cutoff
Fixed Assets	▪ Physical Custody ▪ Asset Accounting ▪ Depreciation ▪ Retirement Obligations ▪ Asset Retirement and Disposal ▪ Project Management

Evaluation of Key Processes (cont.)

Process	Function
Inventory	▪ Physical Custody ▪ Inventory Accounting ▪ Valuation
Information Technology	▪ Logical Access Controls ▪ Program Changes ▪ System Operations ▪ System Migration ▪ Physical and Environmental Controls ▪ Back-up and Recovery ▪ Networks and Communication ▪ Cloud Service Providers ▪ Encryption ▪ System Maintenance/Software Versions ▪ Information Technology Policy Framework ▪ Cybersecurity Preparedness ▪ Graham Leach Bliley Act (GLBA) ▪ Third Party Processors

Evaluation of Key Processes (cont.)

Process	Function
Grant Compliance	▪ Acceptance ▪ Grant Oversight ▪ Compliance ▪ Reporting ▪ Monitoring ▪ Accounting ▪ Billing and Collection ▪ Grant Close Out

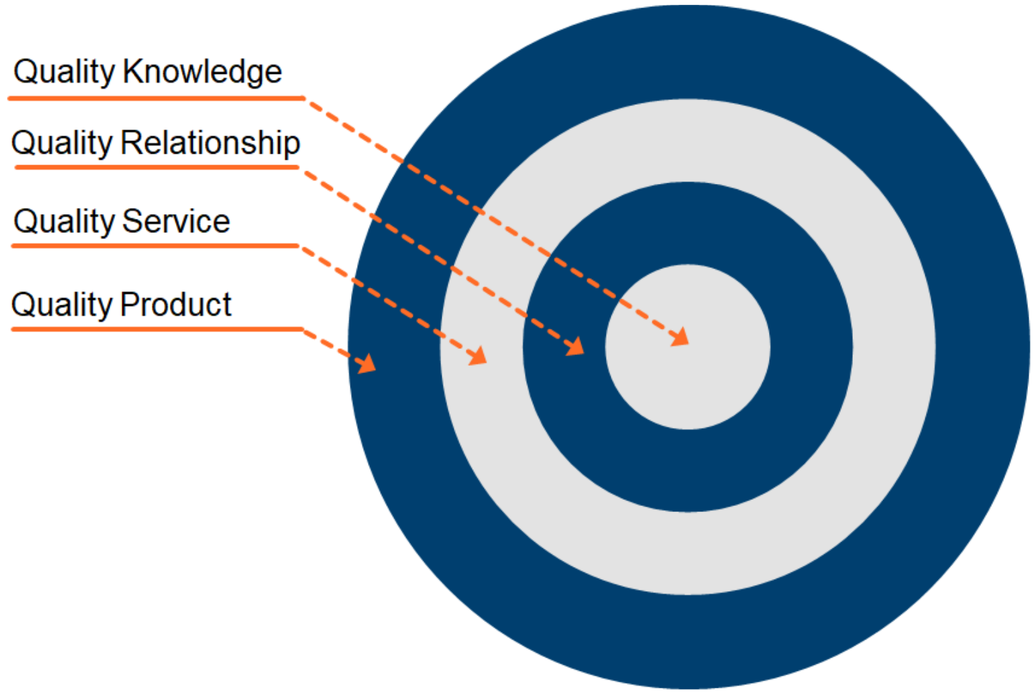
New GASB Pronouncements

- GASB 101 – *Compensated Absences (effective FY2025)*
  - Requires that liabilities for compensated absences be recognized for (1) leave that has not been used and (2) leave that has been used but not yet paid in cash or settled through noncash means.
  - A liability should be recognized for leave that has not been used if (a) the leave is attributable to services already rendered, (b) the leave accumulates, and (c) the leave is more likely than not to be used for time off or otherwise paid in cash or settled through noncash means.
- GASB 102 – *Certain Risk Disclosures (effective FY2025)*
  - Requires a government to assess whether a concentration or constraint makes the primary government reporting unit or other reporting units vulnerable to the risk of a substantial impact and disclose information in notes to financial statements.

New GASB Pronouncements (cont.)

- GASB 103 – *Financial Reporting Models (effective FY2026)*
  - Improve key components of the financial reporting model to enhance its effectiveness in providing information that is essential for decision making and assessing a government's accountability.
  - Outlines requirements for information in and presentation of MD&A, unusual or infrequent items, and Proprietary Fund Statement of Revenues, Expenses, and Changes in Fund Net Position. No significant changes to existing requirements.
- GASB 104 – *Disclosure of Certain Capital Assets (effective FY2026)*
  - Requires certain types of capital assets to be disclosed separately in the capital assets note disclosures required by Statement 34. Lease assets recognized in accordance with Statement No. 87, *Leases*, and intangible right-to-use assets recognized in accordance with Statement No. 94, *Public-Private and Public-Public Partnerships and Availability Payment Arrangements*, should be disclosed separately by major class of underlying asset in the capital assets note disclosures. Subscription assets recognized in accordance with Statement No. 96, *Subscription-Based Information Technology Arrangements*, also should be separately disclosed.
  - Also requires additional disclosures for capital assets held for sale.

SBC Client Service Model



Your Expectations and Communications of Us

Risk areas that are concerns to you	
Prior audit or reporting issues you wanted to discuss with us	
Significant current year transactions and concerns to you	
Expectations of us	
Communications with you	

Engagement Team
Contact Information

Gray Smith, CPA
Client Service/Advisory Partner

Office: 410-584-1401
Cell: 410-340-4515
gsmith@sbandcompany.com

Executive Assistant: Kristina Ortiz
Office: 410-584-9309
kortiz@sbandcompany.com

Monique Booker, CPA
Engagement Partner

Office: 410-584-1403
Cell: 443-804-6129
mbooker@sbandcompany.com

Executive Assistant: Chiami Asemota
Office: 443-705-5076
casemota@sbandcompany.com

Stephen Mackall, CPA
Audit Partner

Office: 410-584-1405
Cell: 443-803-0480
smackall@sbandcompany.com

Executive Assistant: Chiami Asemota
Office: 443-705-5076
casemota@sbandcompany.com

Richard Lee, CPA
Audit Manager

Office: 443-705-5063
Cell: 213-432-1212
richardjlee@sbandcompany.com

Executive Assistant: Kameron Pulliam
Office: 443-353-5437
kpulliam@sbandcompany.com

SBC Knowledge, Quality, Client Service.

Maryland
10200 Grand Central Avenue
Suite 250
Owings Mills, MD 21117
410.584.0060

Washington, D.C.
1200 G Street, NW
Suite 809
Washington, DC 20005
202.434.8684

Information & Discussion – Update of USM Enterprise Risk

TOPIC: Update of USM's Enterprise Risk and Crisis Management Activity

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

SUMMARY:

See attachment

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: none

COMMITTEE ACTION: none DATE:

BOARD ACTION: none DATE:

SUBMITTED BY: David Mosca

University System of Maryland

Update on Enterprise Risk Management

Board of Regents Audit Committee

June 5, 2025

Agenda

- USM ERM Program Update
- Top enterprise risks for the 2024-2025
- Activities since last update

Campus ERM Program Updates - 2025

- 5-6 USM institutions have demonstrated measurable progress in developing their programs.
  - This is supported by the annual updates received in April/May
  - Also, the most recent ERM audits by USM Internal Audit team shows adherence to all audit aspects
- 2-3 institutions are adding dedicated ERM staff to address remaining deficiencies in programs.
- 4-5 institutions are still struggling to get their ERM programs built past the basic risk assessment phase.
- Adoption of ERM into the day-to-day functions of institutions remains a gap for most.

Top Systemwide Risks – 2024-2025

Below are the top enterprise risks by risk category as reported by USM institutions in the 2023-24 reporting period.
Note: Appendix includes anonymized list of all top institutional risks.

High-Level Risk Category	Specific Reported Risks Rated Highest in Total Risk Score (as reported by USM Institutions)
Financial Stability/Sustainability	- **Enrollment/Retention** - **Financial Health/Budget Constraints** - Facilities Infrastructure - Failure to comply with federal, state and USM laws and regulations
Campus Safety	- Near/Campus safety and partnering - Significant student, faculty, staff misconduct - Activism on campus
Information Systems and Data Security	- **Cyber & Data Security and Compliance** - Business continuity – system failure
Quality Educational Experience	- Accreditation requirements - **Attracting and retaining high quality faculty and staff**
Research Funding and Integrity	- Research integrity and security - Growing the research function and creative achievement - **Federal Research Support**

Activities since last update

- ERM representatives met on April 29
  - Discussed proposed changes to ERM policy
  - Planned use of ERM automation tool
- Received and coalesced updates on ERM programs and top risks
- Convened multiple working groups to address budget related enterprise risks

UNIVERSITY SYSTEM
of MARYLAND

Questions

Action, Information & Discussion – Recommended Modification of

TOPIC: Action, Information & Discussion – Proposed Modifications to USM IT Security Standards – Version 5.1

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

During the 2020 Maryland legislative session, SB588/HB1122 passed. These bills place particular security and privacy requirements on all Maryland public higher education institutions, including the USM. In particular, the bills require the following changes:

1. Appendix A – Change to the definition of Personally Identifiable Information and Confidential Information.

2. New Section XI – Creation of a new section on unauthorized access to confidential information.

3. New Line 2.18 – A requirement that the security programs be assessed annually by a third-party assessor.

4. New Line 9.3 – A new requirement that all third-party contracts include a requirement that contractors maintain appropriate security controls commensurate with risk.

The attached draft of 5.1 also includes clerical changes for spelling, updating of names, and clarity. All of the specific changes between version 5.0 and version 5.1.

Attachments.

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: none

COMMITTEE ACTION: None DATE:

BOARD ACTION: None DATE:

SUBMITTED BY: David Mosca

University System of Maryland

Update on Cybersecurity

Board of Regents Audit Committee

June 5, 2025

USM IT Security Standards v5.1

- **Requesting approval of changes to USM IT Security Standards version 5.1**
  - **Reason for Update**
    - SB588/HB1122 (Maryland Higher Education Privacy Act) from the 2020 Maryland legislative session, not only requires changes to our data privacy standards but also has specific IT security requirements.
    - The law went into effect on October 1, 2024.
    - This new version of the USM IT Security Standards incorporates the required changes.

    - The draft before you has been reviewed by the USM CIOs and Security Officers. Their comments have been incorporated into this draft.

Summary of Changes

- **Summary of changes made to Standards 5.0**
  (see attached memo detailing changes)
  - The definitions of confidential information and personally identifiable information were changed to match the definitions of these terms in the 2020 privacy law.
  - A new section was added to the standards to outline the requirements for handling IT security incidents and breaches.
  - A new clause was added to require that institutions periodically have a 3rd party assess their IT security program.
  - A new clause was added to require that institutions take steps to ensure that their 3rd party contracts require outside providers to support the institution's privacy and security programs.
  - Clerical Changes for spelling, updating of names, and clarity.

UNIVERSITY SYSTEM
of MARYLAND

Questions

USM IT SECURITY STANDARDS

Version 5.1

Revised December, 2024

USM IT SECURITY LEADERSHIP:

Lori Bennett, FSU
Christopher Breeden, UB
Mark Cather, USM
Duke Darrigo, SU
Kurt Florez, UMCES
Susan Killian, UMES
Todd Pearce, UMGC
Fred Hayes, USM Office
Malcolm Blow, BSU
Michael Kaiser, TU
Fred Smith, UMB
Gerry Sneeringer, UMCP
Rickey Williams, CSU
Stacy Cahill, UMBC

TABLE OF CONTENTS

I. Introduction

The Board of Regents' Information Technology Policy, in compliance with Section 12-112 of the Education article of the Maryland Code, requires that the University System of Maryland (USM) adopt information technology policies and standards that are functionally compatible with state information technology policies and standards. The Regents' policy was approved in August 2001 and is available at: http://www.usmd.edu/Leadership/BoardOfRegents/Bylaws/SectionX/X100.html

This document addresses security standards established by the state Department of Information Technology (DoIT) for state agencies and interprets those standards in the context of the USM institutions. The state standards are described in the document entitled *Information Security Policy*, which is available on the DoIT website at: http://doit.maryland.gov/policies/Pages/default.aspx

Originally published as a set of guidelines, this document was formally adopted as USM Standards by the Board of Regents on June 27, 2014.

Throughout this document, standards are presented in normal text while commentary and suggestions are presented in italics.

There are a number of references in these standards to NIST Special Publications 800 series documents. These documents are computer security guidelines, recommendations, and reference materials published by the National Institute of Standards and Technology. These documents can be found at https://csrc.nist.gov/publications/sp.

II. IT Security Program Standard

2.1 Institutions must implement a Security Policy and an associated Security Program. The Security Program must be documented and monitored. The CIO or designee must approve institutional security policies. Institutions must periodically assess IT security controls for effectiveness, develop and implement plans for corrective action, and monitor the effectiveness of information security controls on an ongoing basis.

2.2 Procedures required by the USM IT Security Standards must be documented.

2.3 Institutions must have a formal process for the periodic assessment of risk to operations, assets, individuals and reputation, resulting from the operation of information systems and the associated processing, storage, or transmission of confidential information. Once developed, the institutional risk assessment must be reviewed annually for changes in the risk environment; and at least every four years, the institutional risk assessment must be fully updated and revised. The institutional risk assessment process must include identification of systems that process and/or store confidential information, as defined in "Appendix A: Information Classification", and other high-risk systems. Institutional risk assessment processes will be based on the application of the framework in NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. The institutional risk assessment must include a list of systems and other services defined as "high-risk" by the institution.

> *Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgment of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations. Institutions need to recognize that explicit, well-informed risk based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.*

2.4 Institutions will perform an institutional risk assessment and reasonably address the risks posed by confidential information on personal or contractor-owned devices and services.

2.5 Institutions must have documented Change Management procedures in place. Changes with material impact on the security of high-risk IT assets (e.g., firewall rules changes, granting of administrative rights, etc…) must be tracked, reviewed, and approved by a person who does not have a conflict of interest in the approval.

2.6 Institutions must develop and promulgate a Data Classification Policy. The policy must define classes of data that the institution considers to be a risk and the classes of data that the institution does not consider to be a risk. This policy must specify the data that can only be accessed by university-managed devices.

2.7 Institutions must have documented systems (hardware, software, network, or a combination) development lifecycle (SDLC) plans, including the phases of initiation, acquisition/development, baseline configurations and inventories implementation, operations/maintenance, and sunset/disposal. Each phase of the SDLC plan must consider the risks posed by the data and operation of the system and include steps to address any risks in an appropriate manner. This standard applies to high-risk systems as defined by the institution.

The process of developing/acquiring, implementing, operating, and retiring systems (hardware, software, network, or a combination) is known as a System Development Life Cycle (SDLC). See NIST Special Publication 800-160 Volume 1 for helpful guidance.

2.8 Institutions must conduct quarterly vulnerability scans against institutionally-managed high-risk servers and network devices (whether on-premise or in the cloud, consistent with the institutional risk program), and those results must be submitted to USM Internal Audit.

2.9 Institutions must provide security awareness training that covers essential university system and institution-specific security policies and security procedures. All training activities must be documented. At a minimum, the documentation must include the name of the community member, date of training, and information about the training material delivered.

A security awareness program is an essential element of a Security Program. An awareness program should be tailored to address risks identified for an institution's environment.

2.10 Institutions must create an Incident Response Plan based on the "USM IT Incident Response Plan" Template. Incidents involving the compromise of personal information (as defined under State Government Article 10-301, see Section III) or confidential information (as defined in Appendix A of these standards) must be reported to security@usmd.edu.

The USM IT Incident Response Plan Template can be downloaded from: https://itsecurity.usmd.edu

2.11 Institutions must report annually to the senior leadership of the institution on the risk posed to the institution by information technology, cybersecurity, and privacy to the institution. This report must be on record at the institution and must be available upon request from the USM.

2.12 USM institutions must develop acceptable use policies that address the responsible use of institutional computing resources, including electronic mail, network services, electronic documents, information, software, and other resources.

2.13 Each USM institution shall have personnel designated for providing official notices of IT incidents and advisories to the institutional user community. Only these personnel will send such messages.

2.14 Institutions must comply with the Digital Millennium Copyright Act and designate a single point of contact for inquiries about copyright violations.

2.15 Institutions must establish a policy and implement measures to protect Confidential Information from disclosure in conformance with applicable State of Maryland and federal laws. These include having an institutional acceptable use policy, not using confidential information as identifiers, and having an institutional confidentiality/non-disclosure policy or requiring non-disclosure agreements prior to granting employees access to confidential data.

(Note that there is value in reducing the footprint of confidential information in the institution's environment to the extent that this is possible.)

2.16 USM institutions must utilize encryption for Confidential Information and Protected Health Information while the data are in transit or at rest on any media (including portable devices, flash storage, optical media, and magnetic media) or apply compensating controls that are equally secure, depending on the capabilities of the technology in use. When institutions utilize encryption, techniques such as whole disk encryption, file encryption, database encryption, and network-based encryption must be chosen as appropriate to address the risks posed to the institution by the information on the system. Any encryption utilized by an institution must be implemented in a manner which prevents loss of data and ensures continued appropriate access to information and systems. Where applicable and necessary for the institutional risk management program, encryption must be used with 3rd party IT solutions to protect Confidential Information.

(See NIST Special Publication 800-52 Rev.2 for guidance on encryption of data in transit, and FIPS 140-2 for guidance on encryption of data at rest).

2.17 When confidential data are shared with other institutions, the State, or federal agencies, that shared data should be managed with the security requirements determined to be the highest among the sharing institutions involved and approved by the institutional CIO or data steward (i.e. the member of the institution with responsibility for the data).

2.18 Each institution's security program must be periodically assessed by a third-party assessor with expertise in information security.

III. Auditability Standard

3.1 Commensurate with risk, institutions must maintain appropriate audit trails of events and actions related to all on premises and 3rd party IT systems and physical access controls. Audit trails and events must be regularly monitored for indications of suspicious, unusual, unlawful, unauthorized, or inappropriate activity. Signs of compromise or other high-risk events must be immediately reported to appropriate officials for prompt resolution.

Examples of significant events which should be reviewed and documented (where possible) include additions/changes to critical applications, actions performed by administrative level accounts, additions and changes to users' access control profiles, and direct modifications to critical data outside of the application. Where it is not possible to maintain such audit trails, the willingness to accept the risk of not auditing such actions should be documented.

3.2 Institutions must monitor all audit solutions to detect any audit system failures. Any failures of the audit solution must immediately be reported to appropriate officials for prompt resolution.

3.3 All on premises and 3rd party systems must have synchronized clocks so that audit records can be accurately correlated between internal and external systems.

3.4 Access to audit information (e.g. SIEM logs) must be restricted in accordance with the principle of least privilege.

3.5 Commensurate with risk, institutions must utilize SIEM and/or other logging mechanisms to maintain audit trails of events and actions where possible.

IV. Access Control Standard

The Access Control Standard applies to all systems, including those that contain confidential information.

4.1 There must be documented procedures for creating, managing, and rescinding user accounts. At a minimum, these procedures should address:

- The eligibility criteria for obtaining an account
- The processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- The processes for managing the retention of user account information
- All user account access to institutional information technology systems, including access for outside contractors, must be limited based on risk to the institution and the privileges needed to fulfill the institutional roles of the user
- The institution must, at least annually, audit user accounts with access to confidential data to confirm that the privileges granted to each user are appropriate.
- As an individual's relationship to the institution changes, institutions must modify or remove access to systems and information as appropriate based on established processes.

4.2 Institutions must implement authentication and authorization processes that uniquely identify all users and appropriately control access to high-risk systems.

4.3 Prohibit group or shared IDs, unless they are documented as Functional IDs. Where possible, individual accounts should be used to provide accountability for administrative changes. Additionally, non-privileged accounts or roles need to be used when accessing non-administrative functions.

Functional IDs are user accounts associated with a group or role that may be used by multiple individuals or user accounts that are associated with production job processes.

When Functional IDs are issued, the following controls should be in place:

- Eligibility criteria for obtaining an account
- Processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- Processes for managing the retention of user account information

Considering the diverse computing environments at USM institutions, the following password requirements are dependent upon operational capabilities of a particular system. Systems which cannot meet the password requirements below must have a risk assessment in place accepted by the institution and should have mitigating controls in place.

NIST Special Publication 800-63-3 describes the Federal Electronic Authentication (eAuth) Guidelines. eAuth provides a methodology for creating flexible password requirements based upon operational needs and the risks that are present. The process of risk evaluation and how it applies to the selection of requirements can be found in the SP800-63-3 (or later) document.

4.4 For systems utilizing authentication, institutions must implement session locking after an institutionally defined period of inactivity and retain the session lock until access is reestablished using established authentication and authorization procedures.

4.5 Users must adhere to institutional password usage, construction, and change requirements. Systems must comply with EITHER (4.5.a or 4.5.b) AND (4.5.c) below:

a. Meet the eAuth guidelines as outlined in 800-63-3B Section 5.1.1.2 Memorized Secret Authenticators;

or

b. Meet the following alternative requirements:
- Minimum password length: 12 characters
- Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all digits, all special characters, or all alphabetic characters
- Automated controls must ensure that passwords are changed at least annually for general users, and at 90-day intervals for administrative-level accounts
- User IDs associated with a password must be disabled for a period of time after not more than 6 consecutive failed login attempts. A minimum of 10 minutes is required for the reset period

c. Follow the following password management practices:
- Password must not be the same as the user ID
- Store and transmit only encrypted representation of passwords
- Password must not be displayed on screens
- Initial passwords and password resets must be issued pre-expired forcing the user to change the password upon first use
- Password reuse must be limited by not allowing the last 10 passwords to be reused. In addition, password age must be at least 2 days
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established
- Expired passwords must be changed before any other system activity is allowed

4.6 Institutions must either adopt a plan to implement multi-factor authentication (MFA) that includes consideration of high-risk systems and user access privileges, or have MFA in place for such systems.

4.7 The functions of system administration, programming, processing/authorizing business transactions, and security administration must be segregated for high-risk systems. This provides for the appropriate separation of duties. If not possible, compensating controls must be established to mitigate the risk.

4.8 Third party and/or vendor access to high-risk systems must be approved and controlled by the department(s) that directly manage the system or software being accessed.

V. Network Security Standard

5.1 Networked equipment shall be configured and maintained so as to not cause network performance degradation, not cause excessive, unwarranted traffic flows, and be suitably hardened against network security threats.

5.2 Appropriate controls for remote access services (e.g., VPN, VDI, Remote Desktop) must include logging of access and encryption of critical data in-transit.

- Remote access, execution of privileged commands, and any access to confidential data must be authorized prior to allowing connection.
- Remote access must be routed through managed access control points.

5.3 Banner text approved by Legal Counsel must be displayed at all system authentication points where initial user logon occurs, when technically possible and when doing so is not detrimental to the function of the network or system.

5.4 Networks must be protected by firewalls at identified points of interface based on system sensitivity and data classification. Firewalls should be configured to block all unneeded services, prevent direct access to hosts on trusted network from untrusted networks, and maintain audit trails. Management access must be encrypted and limited to designated personnel.

5.5 All network devices (e.g., switches, routers) should have all non-needed services disabled, or have compensating controls in place. Vendor-provided administrator username (if possible) and password must be changed.

5.6 Updates and patches must be installed on all network devices in a timeframe determined based on factors such as risk, interdependence, and/or prevention. Patches deemed "critical" must be installed as soon as possible/practical, no later than quarterly. Justification for delay or non-implementation of critical patches should be documented.

5.7 Implement ingress and egress filtering at the edge of the institution's network to prevent IP spoofing.

5.8 Institutions must establish automated and manual processes for intrusion prevention and/or detection.

- Host-based or network-based, must be utilized
- There must be an escalation plan based on commonly encountered events that include immediate response capability when appropriate
- Limit access to make configuration changes to appropriate personnel as defined by the institution.
- Detection signatures must receive regular updates and remain current.
- If interrogation of encrypted network traffic is not technically feasible, compensating controls must be in place on high-risk systems.

VI. Disaster Recovery & Incident Response Standard

This standard is intended to ensure that USM Institutions have documented procedures in place and are sufficiently prepared to address incidents and unforeseen circumstances which may cause negative impact on a USM institution. The procedures should detail the appropriate response to both Security Incidents and Service Interruptions (e.g. unavailability of mission-critical systems, networks, services, or personnel).

6.1 Institutions shall develop and implement an IT Incident Response Plan and IT Disaster Recovery Plan. Institutions may maintain separate disaster recovery and incident response plans or merge them into one plan. If merged, the required concepts of both types of plans must be included in the one planning document.

6.2 IR Plan Requirements: The IT Incident Response Plan must minimally include the items in the "USM IT Incident Response Plan Template". This template can be downloaded from: https://itsecurity.usmd.edu

6.3 DR Plan Requirements: The IT Disaster Recovery Plan must, at a minimum, include the following:

- Documentation of each high-risk system including:
  - Purpose
  - Software
  - Hardware
  - Operating System
  - Application(s)
  - Data
  - Supporting network infrastructure and communications
  - The contact information for the person or group responsible for the system
- System restoration priority list
- Description of current data back-up and restoration procedures
- Description of back-up storage location(s) or services

See NIST SP 800-34 Rev.1 (Contingency Planning Guide for Federal Information Systems) for additional guidance in developing a Disaster Recovery Plan.

6.4 Institutions must update their IT Incident Response and IT Disaster Recovery Plans annually.

6.5 The institution must test the institution's IT Incident Response Plan at least annually and their disaster recovery plan at least annually. The tests must be documented. If an institution uses their incident response plan or disaster recovery plan to handle a real security or service interruption event, that event may be documented and take the place of the annual test. If a single event or test exercises both the disaster recovery and incident response plans, the one event or test can be used to meet both annual testing requirement.

VII. Physical Security Standard

7.1 Campuses must perform a risk assessment of the physical access controls which are in place protecting the IT facilities (such as server rooms, network closets, and wiring cabinets). Commensurate with this risk assessment, appropriate physical access controls must be in place, such as:

- Maintaining a list of all employees and third parties who are authorized to operate independently and unescorted in secure IT facilities as defined in Section 7.1
- Escorting any individual who is not authorized to operate independently and unescorted in these secure IT facilities and observing their activities at all times while in said facility.
- Ensuring that all portable storage media containing confidential information such as hard drives, flash drives, magnetic tapes, laptops, and CDs are physically secured
- Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of critical information residing on IT systems
- Ensuring that physical access devices are controlled and managed appropriately, and (commensurate with risk) that physical access is auditable.

The following media destruction and reuse standards apply to all electronic storage media equipment that is owned or leased by USM institutions (including, but not limited to: workstations, servers, laptops, cell phones, and multi-function printer/copiers.

7.2 When no longer usable, electronic storage media that contain confidential data shall be destroyed and/or sanitized. Institutions must use methods that are in accordance with the NIST SP800-88rev1 *Guidelines for Media Sanitization.* This requirement applies to the permanent disposal of all storage media and equipment containing storage media regardless of the identity of the recipient. It also applies to equipment sent for maintenance or repair.

7.3 The procedures performed to sanitize electronic media must be documented and data destruction records retained whether performed in-house or by a campus contractor.

7.4 Media must be cleansed in accordance with NIST SP 800-88 before being released internally for reuse. The cleansing technique used should be commensurate with the risk associated with the data stored on that media.

VIII. Endpoint Security Standard

This section applies to Institutionally Owned Devices. These requirements are commensurate with risk and must be applied to the extent that they are practical.

8.1 Controls must be implemented on all endpoints:

- User ID/password, Complex Passcode, Biometric, or other widely accepted authentication technology must be required to access the device.
- Implement appropriate solutions that detect malware and update automatically to identify new threats.
- Host-based firewalls should be operational and properly configured to protect the device when it is outside of the secured institutional network.

8.2 Identify confidential information stored on systems. Where possible and practical, institutions must minimize the storage of confidential information on endpoint systems.

8.3 Implement and document processes for managing exposure to vulnerabilities through the timely deployment of operating system and application patches.

8.4 Using a risk-based approach, implement and document processes that minimize provisioning of local administrative rights so that only those employees who require it are given those rights.

8.5 The institution must establish a procedure for reporting lost/stolen devices and the ability to remotely locate lost/stolen devices.

8.6 The institution must establish a procedure for the remote removal of institutionally-owned data from devices.

IX. Third-Party/Cloud Technology Services Standard

This Standard is intended for USM Institutions that choose to outsource technology services to third-party cloud providers

Examples of third-party cloud technology services include:

- *Cloud Services*
  - *Software-as-a-Service (SaaS)*
  - *Infrastructure -as-a-Service (IaaS)*
  - *Platform-as-a-Service (PaaS)*
  - *Network-as-a-Service (NaaS)*
- *Web Hosting*
- *Application Hosting*
- *Database Hosting*
- *Cloud Data Backup*
- *Offsite Cloud Storage*

Institutions must assess, and take steps to mitigate, the risk of unauthorized access, use, disclosure, modification, or destruction of confidential institutional information. This standard only applies to third-party cloud technology service agreements where there is a potential for high risk to the institution. See Appendix A: Definition of Confidential Information to determine the classification of data involved.

9.1 In conjunction with the Institution's procurement department and security team, stakeholders shall perform the following activities during the life-cycle of the third-party cloud technology service:

- Assess the risks associated with the third-party cloud service. Institutions must ensure that the security of a vendor's cloud solution provides comparable protection to a premises-based solution including the need to ensure confidentiality, integrity, availability, security, and privacy.

- Commensurate with the risk, request and, if available, obtain, review, and document control assessment reports performed by a recognized independent audit organization. Examples of acceptable control assessment reports include (but are not limited to):
  - AICPA SOC2/Type2
  - PCI Security Standards
  - ISO 27001/2 Certification
  - FedRAMP

9.2 Institutions must annually review the most recent control assessment reports as well as the providers' compliance with IT security, privacy, and availability deliverables in the contract. They must also reassess the risk of the cloud solution to ensure that the solution continues to provide adequate protection to institutional information assets.

9.3 Institutions must ensure that contracts with third parties include provisions to ensure that third parties that process personally identifiable information on behalf of the institution maintain appropriate security controls commensurate with the risk posed to the individuals by the personally identifiable information.

9.4 Third-party contracts should include the following as applicable:

- Requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract.
- Service level agreements including provisions for non-compliance.
- Provisions stipulating that the third-party service provider is the owner or authorized user of their software and all of its components, and the third-party's software and all of its components, to the best of third-party's knowledge, do not violate any patent, trademark, trade secret, copyright or any other right of ownership of any other party.
- Provisions that stipulate that all institutional data remains the property of the institution.
- Provisions that require the consent of the institution prior to sharing institutional data with any third parties.
- Provisions that block the secondary use of institutional data.
- Provisions that manage the retention and destruction requirements related to institutional data.
- Provisions that require any vendor to disclose any subcontractors related to their services.
- Requirements to establish and maintain industry standard technical and organizational measures to protect against:
    - accidental destruction, loss, alteration, or damage to the materials;
    - unauthorized access to confidential information
    - unauthorized access to the services and materials; and
    - industry known system attacks (e.g., hacker and virus attacks)
- Requirements for reporting any confirmed or suspected breach of institutional data to the institution.
- Requirements that the institution be given notice of any government or third-party subpoena requests prior to the contractor answering a request.
- The right of the Institution or an appointed audit firm to audit the vendor's security related to the processing, transport, or storage of institutional data.

- Requirement that the Service Provider must periodically make available a third-party review that satisfies the professional requirement of being performed by a recognized independent audit organization (refer to 9.1). In addition, the Service Provider should make available evidence of their business continuity and disaster recovery capabilities to mitigate the impact of a realized risk.
- Requirement that the Service Provider ensure continuity of services in the event of the company being acquired or a change in management.
- Requirement that the contract does not contain the following provisions:
    - The unilateral right of the Service Provider to limit, suspend, or terminate the service (with or without notice and for any reason).
    - A disclaimer of liability for third-party action.
- Requirement that the Service Provider make available audit logs recording privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (as available) [reference Section III – Auditability Standard]

X. Non-Institutionally Owned Devices and Services

Each institution must develop guidelines to govern the use of non-institutionally owned devices (such as personally owned laptops and other computing devices) and non-institutionally purchased/controlled services (such as personally purchased file storage services) for access to institutional resources. These guidelines must address the following areas:

- Risk of confidential data falling into the wrong hands.
- Risk of mission-critical data being lost to the institution (e.g. important research data being outside of the institution's backup scheme).
- Risk of institutional data being stored in non-institutionally purchased/controlled services (e.g. private Google Drive, DropBox, etc.).
- Develop an Institutional Agreement with staff that addresses the following responsibilities of the end-user:
    - Take reasonable steps to secure such a device;
    - Take reasonable steps to secure their home network;
    - Report any potential compromise or loss of the device being used to access institutional resources;
    - Ensure that only an authorized user can use the device to access institutional resources; and
    - Destroy/remove all institutional data upon separation from the institution, or upon the request of the institution.

XI. Unauthorized Access to Confidential Information

Definitions

- "Breach of the security of a system" means the unauthorized acquisition of Confidential Information.
- "Breach of the security of a system" does not include:
    - the good faith acquisition of confidential information by an employee or agent of a public institution of higher education for the purposes of the public institution of higher education, provided that the confidential information is not used or subject to further unauthorized disclosure; or
    - confidential information that was secured by encryption or redacted and for which the encryption key has not been compromised or disclosed.

Investigation: If an institution collects Confidential Information and discovers or is notified of a breach of the security of a system, the institution shall conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personally identifiable information of the individual has occurred.

Notification of Breach: If, after the investigation is concluded, the public institution of higher education determines that a breach of the security of the system has occurred, the public institution of higher education or a third party, if authorized under a written contract or agreement with the public institution of higher education, shall:

- notify the individual of the breach; and
- notify the Chief Information Officer of the public institution of higher education of the breach.

A breach notification shall include, to the extent possible, a description of the categories of personally identifiable information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personally identifiable information were, or are reasonably believed to have been, acquired.
If the institution determines that a breach of the security of the system has occurred involving the personally identifiable information of 1,000 or more individuals, the institution shall post a notice on the same webpage as the institution's privacy notice website describing the breach.

The website breach notice must remain publicly available for at least 1 year from the date on which notice was sent to individuals affected by the breach.

Appendix A: Information Classification

Institutions should organize their policies and procedures based on the following data classifications.

- **Educational Records**: Educational Records as defined and when protected by 20 U.S.C § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades.
- **Protected Health Information**: Any Protected Health Information (PHI) as the term is defined in 45 CFR 160.103 (HIPAA).
- **Personally Identifiable Information**: Any information that, taken alone or in combination with other information, enables the identification of an individual, including:
    - a full name;
    - a Social Security number;
    - a driver's license number, state identification card number, or other individual identification number;
    - a passport number;
    - biometric information including an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity;
    - geolocation data;
    - Internet or other electronic network activity information, including browsing history, search history, and information regarding an individual's interaction with an Internet website, application, or advertisement; and
    - a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.
    - "Personally identifiable information" does not include data rendered anonymous through the use of techniques, including obfuscation, delegation and redaction, and encryption, so that the individual is no longer identifiable.
- **Confidential Information**: Personally Identifiable Information that would pose a reasonable risk of harm to the data subject if accessed or acquired by an unauthorized party.

Additionally, institutions should consider the risk posed by information under the following laws and regulations:

- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission Red Flag Rules
- Payment Card Industry / Data Security Standards (PCI/DSS)
- Maryland Confidentiality of Medical Records Act (MCMRA)

USM IT SECURITY STANDARDS

Version 5.0

Revised June, 2022

USM IT SECURITY COUNCIL:

Lori Bennett, FSU
David Bobart, UB
Mark Cather, UMBC/USM
Duke Darrigo, SU
Michael Eismeier, USM
Kurt Florez, UMES
Cory Gekoski, UMB
Chinitra Graham, UMGC
Fred Hayes, USM
Edward Hodges, UB
Kiki Iyiegbu, BSU
Michael Kaiser, TU
James Kevin Moran, UMSG
Fred Smith, UMB
Gerry Sneeringer, UMCP
Michael Von Paris, TU
Rickey Williams, CSU

TABLE OF CONTENTS

I. Introduction

The Board of Regents' Information Technology Policy, in compliance with Section 12-112 of the Education article of the Maryland Code, requires that the University System of Maryland (USM) adopt information technology policies and standards that are functionally compatible with state information technology policies and standards. The Regents' policy was approved in August 2001 and is available at: http://www.usmd.edu/Leadership/BoardOfRegents/Bylaws/SectionX/X100.html

This document addresses security standards established by the state Department of Information Technology (DoIT) for state agencies and interprets those standards in the context of the USM institutions. The state standards are described in the document entitled *Information Security Policy*, which is available on the DoIT website at: http://doit.maryland.gov/policies/Pages/default.aspx

Originally published as a set of guidelines, this document was formally adopted as USM Standards by the Board of Regents on June 27, 2014.

Throughout this document, standards are presented in normal text while commentary and suggestions are presented in italics.

There are a number of references in these standards to NIST Special Publications 800 series documents. These documents are computer security guidelines, recommendations, and reference materials published by the National Institute of Standards and Technology. These documents can be found at https://csrc.nist.gov/publications/sp.

II. IT Security Program Standard

2.1 Institutions must implement a Security Policy and an associated Security Program. The Security Program must be documented and monitored. The CIO or designee must approve institutional security policies. Institutions must periodically assess IT security controls for effectiveness, develop and implement plans for corrective action, and monitor the effectiveness of information security controls on an ongoing basis.

2.2 Procedures required by the USM IT Security Standards must be documented.

2.3 Institutions must have a formal process for the periodic assessment of risk to operations, assets, individuals and reputation, resulting from the operation of information systems and the associated processing, storage, or transmission of confidential information. Once developed, the institutional risk assessment must be reviewed annually for changes in the risk environment; and at least every four years, the institutional risk assessment must be fully updated and revised. The institutional risk assessment process must include identification of systems that process and/or store confidential information, as defined in "Appendix A: Information Classification", and other high-risk systems. Institutional risk assessment processes will be based on the application of the framework in NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. The institutional risk assessment must include a list of systems and other services defined as "high-risk" by the institution.

Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgment of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations. Institutions need to recognize that explicit, well-informed risk based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.

2.4 Institutions will perform an institutional risk assessment and reasonably address the risks posed by confidential information on personal or contractor-owned devices and services.

2.5 Institutions must have documented Change Management procedures in place. Changes with material impact on the security of high-risk IT assets (e.g., firewall rules changes, granting of administrative rights, etc…) must be tracked, reviewed, and approved by a person who does not have a conflict of interest in the approval.

2.6 Institutions must develop and promulgate a Data Classification Policy. The policy must define classes of data that the institution considers to be a risk and the classes

of data that the institution does not consider to be a risk. This policy must specify the data that can only be accessed by university-managed devices.

2.7 Institutions must have documented systems (hardware, software, network, or a combination) development lifecycle (SDLC) plans, including the phases of initiation, acquisition/development, baseline configurations and inventories implementation, operations/maintenance, and sunset/disposal. Each phase of the SDLC plan must consider the risks posed by the data and operation of the system and include steps to address any risks in an appropriate manner. This standard applies to high-risk systems as defined by the institution.

The process of developing/acquiring, implementing, operating, and retiring systems (hardware, software, network, or a combination) is known as a System Development Life Cycle (SDLC). See NIST Special Publication 800-160 Volume 1 for helpful guidance.

2.8 Institutions must conduct quarterly vulnerability scans against institutionally-managed high-risk servers and network devices (whether on-premise or in the cloud, consistent with the institutional risk program), and those results must be submitted to USM Internal Audit.

2.9 Institutions must provide security awareness training that covers essential university system and institution-specific security policies and security procedures. All training activities must be documented. At a minimum, the documentation must include the name of the community member, date of training, and information about the training material delivered.

A security awareness program is an essential element of a Security Program. An awareness program should be tailored to address risks identified for an institution's environment.

2.10 Institutions must create an Incident Response Plan based on the "USM IT Incident Response Plan" Template. Incidents involving the compromise of personal information (as defined under State Government Article 10-301, see Section III) or confidential information (as defined in Appendix A of these standards) must be reported to security@usmd.edu.

The USM IT Incident Response Plan Template can be downloaded from: https://itsecurity.usmd.edu

2.11 Institutions must report annually to the senior leadership of the institution on the risk posed to the institution by information technology, cybersecurity, and privacy to the institution. This report must be on record at the institution and must be available upon request from the USM.

2.12 USM institutions must develop acceptable use policies that address the responsible use of institutional computing resources, including electronic mail, network services, electronic documents, information, software, and other resources.

2.13 Each USM institution shall have personnel designated for providing official notices of IT incidents and advisories to the institutional user community. Only these personnel will send such messages.

2.14 Institutions must comply with the Digital Millennium Copyright Act and designate a single point of contact for inquiries about copyright violations.

2.15 Institutions must establish a policy and implement measures to protect Confidential Information from disclosure in conformance with applicable State of Maryland and federal laws. These include having an institutional acceptable use policy, not using confidential information as identifiers, and having an institutional confidentiality/non-disclosure policy or requiring non-disclosure agreements prior to granting employees access to confidential data.

(Note that there is value in reducing the footprint of confidential information in the institution's environment to the extent that this is possible.)

2.16 USM institutions must utilize encryption for Confidential Information and Protected Health Information while the data are in transit or at rest on any media (including portable devices, flash storage, optical media, and magnetic media) or apply compensating controls that are equally secure, depending on the capabilities of the technology in use. When institutions utilize encryption, techniques such as whole disk encryption, file encryption, database encryption, and network-based encryption must be chosen as appropriate to address the risks posed to the institution by the information on the system. Any encryption utilized by an institution must be implemented in a manner which prevents loss of data and ensures continued appropriate access to information and systems. Where applicable and necessary for the institutional risk management program, encryption must be used with 3rd party IT solutions to protect Confidential Information.

(See NIST Special Publication 800-52 Rev.2 for guidance on encryption of data in transit, and FIPS 140-2 for guidance on encryption of data at rest).

2.17 When confidential data are shared with other institutions, the State, or federal agencies, that shared data should be managed with the security requirements determined to be the highest among the sharing institutions involved and approved by the institutional CIO or data steward (i.e. the member of the institution with responsibility for the data).

III. Auditability Standard

3.1 Commensurate with risk, institutions must maintain appropriate audit trails of events and actions related to all on premises and 3rd party IT systems and physical access controls. Audit trails and events must be regularly monitored for indications of suspicious, unusual, unlawful, unauthorized, or inappropriate activity. Signs of compromise or other high-risk events must be immediately reported to appropriate officials for prompt resolution.

Examples of significant events which should be reviewed and documented (where possible) include additions/changes to critical applications, actions performed by administrative level accounts, additions and changes to users' access control profiles, and direct modifications to critical data outside of the application. Where it is not possible to maintain such audit trails, the willingness to accept the risk of not auditing such actions should be documented.

3.2 Institutions must monitor all audit solutions to detect any audit system failures. Any failures of the audit solution must immediately be reported to appropriate officials for prompt resolution.

3.3 All on premises and 3rd party systems must have synchronized clocks so that audit records can be accurately correlated between internal and external systems.

3.4 Access to audit information (e.g. SIEM logs) must be restricted in accordance with the principal of least privilege.

3.5 Commensurate with risk, institutions must utilize SIEM and/or other logging mechanisms to maintain audit trails of events and actions where possible.

IV. Access Control Standard

The Access Control Standard applies to all systems, including those that contain confidential information.

4.1 There must be documented procedures for creating, managing, and rescinding user accounts. At a minimum, these procedures should address:

- The eligibility criteria for obtaining an account
- The processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- The processes for managing the retention of user account information
- All user account access to institutional information technology systems, including access for outside contractors, must be limited based on risk to the institution and the privileges needed to fulfill the institutional roles of the user
- The institution must, at least annually, audit user accounts with access to confidential data to confirm that the privileges granted to each user are appropriate.
- As an individual's relationship to the institution changes, institutions must modify or remove access to systems and information as appropriate based on established processes.

4.2 Institutions must implement authentication and authorization processes that uniquely identify all users and appropriately control access to high-risk systems.

4.3 Prohibit group or shared IDs, unless they are documented as Functional IDs. Where possible, individual accounts should be used to provide accountability for administrative changes. Additionally, non-privileged accounts or roles need to be used when accessing non-administrative functions.

Functional IDs are user accounts associated with a group or role that may be used by multiple individuals or user accounts that are associated with production job processes.

When Functional IDs are issued, the following controls should be in place:

- Eligibility criteria for obtaining an account
- Processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- Processes for managing the retention of user account information

Considering the diverse computing environments at USM institutions, the following password requirements are dependent upon operational capabilities of a particular system. Systems which cannot meet the password requirements below must have a risk assessment in place accepted by the institution and should have mitigating controls in place.

NIST Special Publication 800-63-3 describes the Federal Electronic Authentication (eAuth) Guidelines. eAuth provides a methodology for creating flexible password requirements based upon operational needs and the risks that are present. The process of risk evaluation and how it applies to the selection of requirements can be found in the SP800-63-3 (or later) document.

4.4 For systems utilizing authentication, institutions must implement session locking after an institutionally defined period of inactivity and retain the session lock until access is reestablished using established authentication and authorization procedures.

4.5 Users must adhere to institutional password usage, construction, and change requirements. Systems must comply with EITHER (4.5.a or 4.5.b) AND (4.5.c) below:

a. Meet the eAuth guidelines as outlined in 800-63-3B Section 5.1.1.2 Memorized Secret Authenticators;

or

b. Meet the following alternative requirements:
- Minimum password length: 12 characters
- Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all digits, all special characters, or all alphabetic characters
- Automated controls must ensure that passwords are changed at least annually for general users, and at 90-day intervals for administrative-level accounts
- User IDs associated with a password must be disabled for a period of time after not more than 6 consecutive failed login attempts. A minimum of 10 minutes is required for the reset period

c. Follow the following password management practices:
- Password must not be the same as the user ID
- Store and transmit only encrypted representation of passwords
- Password must not be displayed on screens
- Initial passwords and password resets must be issued pre-expired forcing the user to change the password upon first use
- Password reuse must be limited by not allowing the last 10 passwords to be reused. In addition, password age must be at least 2 days
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established
- Expired passwords must be changed before any other system activity is allowed

4.6 Institutions must either adopt a plan to implement multi-factor authentication (MFA) that includes consideration of high-risk systems and user access privileges, or have MFA in place for such systems.

4.7 The functions of system administration, programming, processing/authorizing business transactions, and security administration must be segregated for high-risk systems. This provides for the appropriate separation of duties. If not possible, compensating controls must be established to mitigate the risk.

4.8 Third party and/or vendor access to high-risk systems must be approved and controlled by the department(s) that directly manage the system or software being accessed.

V. Network Security Standard

5.1 Networked equipment shall be configured and maintained so as to not cause network performance degradation, not cause excessive, unwarranted traffic flows, and be suitably hardened against network security threats.

5.2 Appropriate controls for remote access services (e.g., VPN, VDI, Remote Desktop) must include logging of access and encryption of critical data in-transit.

- Remote access, execution of privileged commands, and any access to confidential data must be authorized prior to allowing connection.
- Remote access must be routed through managed access control points.

5.3 Banner text approved by Legal Counsel must be displayed at all system authentication points where initial user logon occurs, when technically possible and when doing so is not detrimental to the function of the network or system.

5.4 Networks must be protected by firewalls at identified points of interface based on system sensitivity and data classification. Firewalls should be configured to block all unneeded services, prevent direct access to hosts on trusted network from untrusted networks, and maintain audit trails. Management access must be encrypted and limited to designated personnel.

5.5 All network devices (e.g., switches, routers) should have all non-needed services disabled, or have compensating controls in place. Vendor-provided administrator username (if possible) and password must be changed.

5.6 Updates and patches must be installed on all network devices in a timeframe determined based on factors such as risk, interdependence, and/or prevention. Patches deemed "critical" must be installed as soon as possible/practical, no later than quarterly. Justification for delay or non-implementation of critical patches should be documented.

5.7 Implement ingress and egress filtering at the edge of the institution's network to prevent IP spoofing.

5.8 Institutions must establish automated and manual processes for intrusion prevention and/or detection.

- Host-based or network-based, must be utilized
- There must be an escalation plan based on commonly encountered events that include immediate response capability when appropriate
- Limit access to make configuration changes to appropriate personnel as defined by the institution.
- Detection signatures must receive regular updates and remain current.
- If interrogation of encrypted network traffic is not technically feasible, compensating controls must be in place on high-risk systems.

VI. Disaster Recovery & Incident Response Standard

This standard is intended to ensure that USM Institutions have documented procedures in place and are sufficiently prepared to address incidents and unforeseen circumstances which may cause negative impact on a USM institution. The procedures should detail the appropriate response to both Security Incidents and Service Interruptions (e.g. unavailability of mission-critical systems, networks, services, or personnel).

6.1 Institutions shall develop and implement an IT Incident Response Plan and IT Disaster Recovery Plan. Institutions may maintain separate disaster recovery and incident response plans or merge them into one plan. If merged, the required concepts of both types of plans must be included in the one planning document.

6.2 IR Plan Requirements: The IT Incident Response Plan must minimally include the items in the "USM IT Incident Response Plan Template". This template can be downloaded from: https://itsecurity.usmd.edu

6.3 DR Plan Requirements: The IT Disaster Recovery Plan must, at a minimum, include the following:

- Documentation of each high-risk system including:
  - Purpose
  - Software
  - Hardware
  - Operating System
  - Application(s)
  - Data
  - Supporting network infrastructure and communications
  - The contact information for the person or group responsible for the system
- System restoration priority list
- Description of current data back-up and restoration procedures
- Description of back-up storage location(s) or services

See NIST SP 800-34 Rev.1 (Contingency Planning Guide for Federal Information Systems) for additional guidance in developing a Disaster Recovery Plan.

6.4 Institutions must update their IT Incident Response and IT Disaster Recovery Plans annually.

6.5 The institution must test the institution's IT Incident Response Plan at least annually and their disaster recovery plan at least annually. The tests must be documented. If an institution uses their incident response plan or disaster recovery plan to handle a real security or service interruption event, that event may be documented and take the place of the annual test. If a single event or test exercises both the disaster recovery and incident response plans, the one event or test can be used to meet both annual testing requirement.

VII. Physical Security Standard

7.1 Campuses must perform a risk assessment of the physical access controls which are in place protecting the IT facilities (such as server rooms, network closets, and wiring cabinets). Commensurate with this risk assessment, appropriate physical access controls must be in place, such as:

- Maintaining a list of all employees and third parties who are authorized to operate independently and unescorted in secure IT facilities as defined in Section 7.1
- Escorting any individual who is not authorized to operate independently and unescorted in these secure IT facilities and observing their activities at all times while in said facility.
- Ensuring that all portable storage media containing confidential information such as hard drives, flash drives, magnetic tapes, laptops, and CDs are physically secured
- Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of critical information residing on IT systems
- Ensuring that physical access devices are controlled and managed appropriately, and (commensurate with risk) that physical access is auditable.

The following media destruction and reuse standards apply to all electronic storage media equipment that is owned or leased by USM institutions (including, but not limited to: workstations, servers, laptops, cell phones, and multi-function printer/copiers.

7.2 When no longer usable, electronic storage media that contain confidential data shall be destroyed and/or sanitized. Institutions must use methods that are in accordance with the NIST SP800-88rev1 *Guidelines for Media Sanitization.* This requirement applies to the permanent disposal of all storage media and equipment containing storage media regardless of the identity of the recipient. It also applies to equipment sent for maintenance or repair.

7.3 The procedures performed to sanitize electronic media must be documented and data destruction records retained whether performed in-house or by a campus contractor.

7.4 Media must be cleansed in accordance with NIST SP 800-88 before being released internally for reuse. The cleansing technique used should be commensurate with the risk associated with the data stored on that media.

VIII. Endpoint Security Standard

This section applies to Institutionally Owned Devices. These requirements are commensurate with risk and must be applied to the extent that they are practical.

8.1 Controls must be implemented on all endpoints:

- User ID/password, Complex Passcode, Biometric, or other widely accepted authentication technology must be required to access the device.
- Implement appropriate solutions that detect malware and update automatically to identify new threats.
- Host-based firewalls should be operational and properly configured to protect the device when it is outside of the secured institutional network.

8.2 Identify confidential information stored on systems. Where possible and practical, institutions must minimize the storage of confidential information on endpoint systems.

8.3 Implement and document processes for managing exposure to vulnerabilities through the timely deployment of operating system and application patches.

8.4 Using a risk-based approach, implement and document processes that minimize provisioning of local administrative rights so that only those employees who require it are given those rights.

8.5 The institution must establish a procedure for reporting lost/stolen devices and the ability to remotely locate lost/stolen devices.

8.6 The institution must establish a procedure for the remote removal of institutionally-owned data from devices.

IX. Third-Party/Cloud Technology Services Standard

This Standard is intended for USM Institutions that choose to outsource technology services to third-party cloud providers

Examples of third-party cloud technology services include:

- *Cloud Services*
  - *Software-as-a-Service (SaaS)*
  - *Infrastructure -as-a-Service (IaaS)*
  - *Platform-as-a-Service (PaaS)*
  - *Network-as-a-Service (NaaS)*
- *Web Hosting*
- *Application Hosting*
- *Database Hosting*
- *Cloud Data Backup*
- *Offsite Cloud Storage*

Institutions must assess, and take steps to mitigate, the risk of unauthorized access, use, disclosure, modification, or destruction of confidential institutional information. This standard only applies to third-party cloud technology service agreements where there is a potential for high risk to the institution. See Appendix A: Definition of Confidential Information to determine the classification of data involved.

9.1 In conjunction with the Institution's procurement department and security team, stakeholders shall perform the following activities during the life-cycle of the third-party cloud technology service:

- Assess the risks associated with the third-party cloud service. Institutions must ensure that the security of a vendor's cloud solution provides comparable protection to a premises-based solution including the need to ensure confidentiality, integrity, availability, security, and privacy.

- Commensurate with the risk, request and, if available, obtain, review, and document control assessment reports performed by a recognized independent audit organization. Examples of acceptable control assessment reports include (but are not limited to):
  - AICPA SOC2/Type2
  - PCI Security Standards
  - ISO 27001/2 Certification
  - FedRAMP

9.2 Institutions must annually review the most recent control assessment reports as well as the providers' compliance with IT security, privacy, and availability deliverables

in the contract. They must also reassess the risk of the cloud solution to ensure that the solution continues to provide adequate protection to institutional information assets.

9.3 Third-party contracts should include the following as applicable:

- Requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract.
- Service level agreements including provisions for non-compliance.
- Provisions stipulating that the third-party service provider is the owner or authorized user of their software and all of its components, and the third-party's software and all of its components, to the best of third-party's knowledge, do not violate any patent, trademark, trade secret, copyright or any other right of ownership of any other party.
- Provisions that stipulate that all institutional data remains the property of the institution.
- Provisions that require the consent of the institution prior to sharing institutional data with any third parties.
- Provisions that block the secondary use of institutional data.
- Provisions that manage the retention and destruction requirements related to institutional data.
- Provisions that require any vendor to disclose any subcontractors related to their services.
- Requirements to establish and maintain industry standard technical and organizational measures to protect against:
    - accidental destruction, loss, alteration, or damage to the materials;
    - unauthorized access to confidential information
    - unauthorized access to the services and materials; and
    - industry known system attacks (e.g., hacker and virus attacks)
- Requirements for reporting any confirmed or suspected breach of institutional data to the institution.
- Requirements that the institution be given notice of any government or third-party subpoena requests prior to the contractor answering a request.
- The right of the Institution or an appointed audit firm to audit the vendor's security related to the processing, transport, or storage of institutional data.
- Requirement that the Service Provider must periodically make available a third-party review that satisfies the professional requirement of being performed by a recognized independent audit organization (refer to 9.1). In addition, the Service Provider should make available evidence of their business continuity and disaster recovery capabilities to mitigate the impact of a realized risk.
- Requirement that the Service Provider ensure continuity of services in the event of the company being acquired or a change in management.
- Requirement that the contract does not contain the following provisions:

    - The unilateral right of the Service Provider to limit, suspend, or terminate the service (with or without notice and for any reason).
    - A disclaimer of liability for third-party action.
- Requirement that the Service Provider make available audit logs recording privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (as available) [reference Section III – Auditability Standard]

X. Policy on Non-Institutionally-Owned Devices and Services

Each institution must develop guidelines to govern the use of non-institutionally owned devices (such as personally owned laptops and other computing devices) and non-institutionally purchased/controlled services (such as personally purchased file storage services) for access to institutional resources. These guidelines must address the following areas:

- Risk of confidential data falling into the wrong hands.
- Risk of mission-critical data being lost to the institution (e.g. important research data being outside of the institution's backup scheme).
- Risk of institutional data being stored in non-institutionally purchased/controlled services (e.g. private Google Drive, DropBox, etc.).
- Develop an Institutional Agreement with staff that addresses the following responsibilities of the end-user:
    - Take reasonable steps to secure such a device;
    - Take reasonable steps to secure their home network;
    - Report any potential compromise or loss of the device being used to access institutional resources;
    - Ensure that only an authorized user can use the device to access institutional resources; and
    - Destroy/remove all institutional data upon separation from the institution, or upon the request of the institution.

Appendix A: Information Classification

Institutions should organize their policies and procedures based on the following data classifications.

- Educational Records: Educational Records as defined and when protected by 20 U.S.C § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades.
- Protected Health Information: Any Protected Health Information (PHI) as the term is defined in 45 CFR 160.103 (HIPAA).
- Confidential Information: Personal information as defined in the Maryland Code under State Government Article, §10-1301 - §10-1308:

  An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

  i. a social security number;
  ii. a driver's license number, state identification card number, or other individual identification number issued by a unit;
  iii. a passport number or other identification number issued by the United States government;
  iv. an individual taxpayer identification number; or
  v. a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

Additionally, institutions should consider the risk posed by information under the following laws and regulations:

i. Gramm-Leach-Bliley Act (GLBA)
ii. Federal Trade Commission Red Flag Rules
iii. Payment Card Industry / Data Security Standards (PCI/DSS)
iv. Maryland Confidentiality of Medical Records Act (MCMRA)

Information & Discussion – Review of Presidents, Chancellor, and Board

TOPIC: Review of Presidents', Chancellor's and Regents' Financial Disclosure Forms

COMMITTEE: Audit

DATE OF BOARD OF REGENTS MEETING: June 5, 2025

In accordance with Md. Education Code Ann. §12-104(p), the Board of Regents (BOR) Bylaws and the BOR Committee on Audit's Charter, the Office of Internal Audit has completed its review of the calendar year 2024 financial disclosure statements from the University Presidents (Attachment A), the Chancellor (Attachment A) and the Board of Regents (Attachment B).

The following subjects make up the reporting requirements, which are also summarized in attachments A and B. There are no sections J through W.

Schedule A: Real Property (This section is not required to be completed by the Regents)

You must disclose:

1. Property owned directly, both commercial and residential.
2. Property leased or rented as a tenant, both commercial and residential.
3. A place of residence without a formal agreement, if you provided any monetary contributions to the household.
4. Property owned jointly or through a partnership, limited liability partnership, or limited company in which you held an interest.

Schedule B: Securities (This section is not required to be completed by the Regents)

You must disclose:

1. Shares of stock you own directly or as a part of an Individual Retirement Account (IRA), including a Roth IRA.
2. Bonds issued by corporate entities.
3. Mutual funds and exchange-traded funds (ETFs), ONLY IF they consist primarily of holdings and stock interests in a specific sector regulated by your governmental unit.

Schedule C: Ownership in Business Entities

You must report each interest you held during the reporting period, in business entities that you owned in whole or part, directly or indirectly, jointly and severally, WHETHER OR NOT that entity did business with the State. Pursuant to §5-607(a-1) of the Public Ethics Law, an individual who is required to disclose the name of a business under this section shall disclose any other names that the business is trading as or doing business as. This schedule concerns the reporting of ownership in business entities, other than stocks (which are reported on Schedule B).

You must disclose ownership in a:

1. Corporation
2. Partnership
3. Limited liability partnership (LLP) (Limited Liability Partnership)
4. Limited liability company (LLC) (Limited Liability Company)
5. Sole proprietorship

You are not required to disclose ownership in a sole proprietorship if:

1. The entity did not do business with the State; **AND**
2. You did not earn an income from the entity.

Schedule D: Gifts

You must report each gift you received during the reporting period, along with all gifts given to another person at your direction. You are not required to report a gift received from a member of your immediate family or your parent(s), or any kind of political campaign contributions. Please answer all questions related to each gift or upload a listing of all your gifts with their complete description.
You must disclose gifts with a value of more than $20, or multiple gifts from the same donor if the gifts had a cumulative value of $100 or more. Include gifts from:

1. A regulated lobbyist;
2. An entity engaged in activity regulated or controlled by the State;
3. An entity that otherwise did business with the State; or
4. An association or any entity acting on behalf of an association that is engaged only in representing counties or municipal corporations.

For Legislative Staff ONLY:
You need not disclose if you attended a special meal or reception to which a qualifying legislative unit (i.e. all members, either house, a standing committee or a county or regional delegation officially designated for disclosure purposes by the presiding officers) was invited, and the meal/beverage was consumed in the presence of the donor or sponsor.

Schedule E: Debts and Liabilities

You must disclose:

1. Debts you owe to entities if they did business by sales, purchases, contract, or lease of at least $5,000 with your governmental unit during the reporting period.
    - Typical debts to report are installment loans, mortgages, car loans, or other time-fixed liabilities owed to financial institutions such as banks, credit unions, mortgage companies, and similar entities.
    - Other reportable debts could include those owed to other entities, including merchants, contractors, etc.
2. Debts you owe to entities if the entity was regulated by your governmental unit *Example: Department of Labor, Licensing, and Regulation (DLLR) filers must disclose mortgages owed to financial institutions regulated by the Commissioner of Financial Regulation as that Office is within DLLR.*
3. Debts you owe to regulated lobbyists.
4. Debts your spouse owes, ONLY IF you were involved in the transaction that gave rise to the debt.
5. Debts your dependent children owe, ONLY IF you were involved in the transaction that gave rise to the debt.

Schedule F: Employment and Offices Held

You must disclose:

1. Any outside employment where you earned a salary, WHETHER OR NOT your employer did business with the State.
2. Any unsalaried positions you held, such as an officer or director of a for-profit or not-for-profit organization, but ONLY IF the entity did business with the State.

Schedule G: Spouse

You must report each place of salaried employment held by your spouse during the reporting period, WHETHER OR NOT your spouse's employer did business with the State. You must also report unsalaried offices, directorships, or similar positions for your spouse with any entity that did business with the State. You must also report any solely or partially owned business from which your spouse earned income.

Lobbying Disclosure: If your spouse was a regulated lobbyist with the State during the reporting period, you must also identify each client that engaged your spouse for lobbying purposes.

Schedule H: Dependent Children

You must report each place of salaried employment held by your dependent children during the reporting period, subject to the conditions below. You must also report unsalaried offices, directorships, or similar positions for your dependent children with any entity that did business with the State. You must also report any solely or partially owned business from which your children earned income.

The statement may not include a minor child's employment or business interests unless the employment or business interests are with:

1. The State.
2. An entity regulated by your governmental unit.
3. An entity that has contracts in excess of $10,000 with your governmental unit.

Schedule I: Relationship with State or Local Government, Quasi-Governmental Entity or University of Maryland Medical System (UMMS)

You must report any and all relationships with UMMS, a governmental entity of the State or a local government in the State, or a **quasi-governmental** entity of the State or local government in the State. For each interest disclosed, including any **attributable** interest, please include the name of the agency, the services performed, and the consideration earned from the financial relationship.

For the purposes of this schedule, a relationship is defined as:

1. Any receipt of compensation for representation of UMMS, a governmental entity of the State or a local government in the State, or a **quasi-governmental** entity of the State or local government in the State.
2. Any financial or contractual relationship, with UMMS, a governmental entity of the State or a local government in the State, or a **quasi-governmental** entity of the State or local government in the State.
3. Any transaction with UMMS, a governmental entity of the State or a local government in the State, or a **quasi-governmental** entity of the State or local government in the State, involving a monetary consideration.

Schedule X: Other

Schedule X is an optional schedule if you have other interests or transactions that have not been disclosed on the previous schedules and which you feel should be disclosed. This is also the chance to add more explanation or clarification to any of your responses on other schedules.

If you served as a member of a State board or commission during the reporting period, please list the name of that board or commission.

(Attachments)

FISCAL IMPACT: none

CHANCELLOR'S & COMMITTEE ON AUDIT'S RECOMMENDATION:

BOARD ACTION none DATE:
SUBMITTED BY: COMMITTEE ON AUDIT

The University System of Maryland
Office of Internal Audit
Summarized Review of State Ethics Commission Financial Disclosures - USM Chancellor & Presidents
Calendar Year 2024

		Disclosure Sections									
		A	B	C	D	E	F	G	H	I	X
		Real Property	Securities	Business Ownership	Gifts	Debts & Liabilities	Employment and Offices Held	Spouse	Dependent Children	Relationship with Govt. or UMMS	Other
Dr. Heidi Anderson		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Dr. Aminta H. Breaux		Y	Y	N/A	Y	Y	Y	N/A	N/A	N/A	N/A
Mr. Albert Delia		Y	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Dr. William Dennison		Y	N/A	Y	N/A	N/A	Y	N/A	N/A	N/A	N/A
Dr. Gregory W Fowler		Y	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A	N/A
Dr. Mark Ginsberg		Y	Y	N/A	N/A	N/A	Y	Y	N/A	N/A	N/A
Dr. Bruce Jarrell		Y	Y	N/A	N/A	N/A	Y	N/A	N/A	Y	N/A
Dr. Anthony Jenkins		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Dr. Fernando Miralles-Wilhelm		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Dr. Jay Perman		Y	Y	N/A	N/A	Y	Y	N/A	N/A	N/A	N/A
Dr. Darryll Pines		Y	Y	Y	N/A	N/A	Y	Y	N/A	N/A	N/A
Dr. Carolyn Ringer Lepre		N/A	N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A
Hon. Kurt Schmoke		Y	Y	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A
Dr. Valerie Sheares Ashby		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Y = Included a Disclosure(s)
N/A = No Disclosure was Made

Auditor's Note - There were no inappropriate conflicts of interests or inappropriate disclosures identified in any of the forms reviewed.
Auditor's Note 2 - There are no sections J - W in the Financial Disclosure Form

The University System of Maryland
Office of Internal Audit
Summarized Review of State Ethics Commission Financial Disclosures - USM Regents
Calendar Year 2024

		Disclosure Sections									
		A	B	C	D	E	F	G	H	I	X
		Real Property	Securities	Business Ownership	Gifts	Debts & Liabilities	Employment and Offices Held	Spouse	Dependent Children	Relationship with Govt. or UMMS	Other
Kevin Anderson		Y	N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	Y
Kevin Atticks		Y	Y	Y	N/A	N/A	Y	Y	N/A	N/A	N/A
Hugh Breslin		N/A	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Ellen Rafferty Fish		N/A	N/A	N/A	N/A	N/A	Y	Y	Y	Y	N/A
Goeffrey J. Gonella		Y	N/A	Y	N/A	N/A	Y	Y	N/A	Y	Y
Linda R. Gooden		N/A	Y	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Michelle Gourdine		N/A	N/A	N/A	N/A	N/A	Y	Y	N/A	N/A	N/A
Anwer Hasan		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Farah Helal		N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Robert Hur		N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Isiah Leggett		Y	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yvette Lewis		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Charles McMillen		N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Dhruvak Mirani		N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	Y	N/A
Yehuda Neuberger		N/A	N/A	Y	N/A	N/A	N/A	Y	N/A	N/A	N/A
Josiah Parker		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Louis M. Pope		N/A	N/A	Y	N/A	N/A	Y	N/A	N/A	N/A	N/A

Robert D. Rauch		Y	Y	Y	N/A	Y	Y	Y	N/A	N/A	N/A
Steven Sibel		N/A	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Andrew Smarick		N/A	N/A	N/A	N/A	N/A	Y	Y	N/A	N/A	N/A
William T. Wood		N/A	N/A	Y	N/A	N/A	Y	N/A	N/A	Y	N/A

Y = Included a Disclosure(s)
N/A = No Disclosure was Made

Auditor's Note - There were no inappropriate conflicts of interests or inappropriate disclosures identified in any of the forms reviewed.
Auditor's Note 2 - There are no sections J - W in the Financial Disclosure Form

Information & Discussion - Follow up of Action Items from Previous

TOPIC: Follow up of Action Items from Prior Audit Committee Meetings

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

SUMMARY:

Attachment: Register of Open Action Items from Prior Audit Committee Meetings.

attachment

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: none

COMMITTEE ACTION: none DATE:

BOARD ACTION: none DATE:

SUBMITTED BY: David Mosca

USM Board of Regents
Action Items From Prior Audit Committee Meetings
5-Jun-25

From March 2025 Audit Committee Meeting

	Action Item	Status
1.	Monitor BSU's student accounts recievables.	Ongoing.

From June 2024 Audit Committee Meeting

1.	Monitor Progress of UMGC's OLA audit results.	Update provided for October 2024 an December 2024 Audit Committee meetings. Update to be provided at the June 2025 meeting.

From April 2024 Audit Committee Meeting

1.	Invite Mandiant to make a presentation to audit committee at a future meeting. Include discussion regarding vulnerability trends.	In process.

Note: Action items concluded prior to the June 2024 BOR Audit Committee meeting are not included in this schedule.

Approval - Convene to Closed Session

UNIVERSITY SYSTEM of MARYLAND

BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION, INFORMATION OR DISCUSSION

TOPIC: Convening Closed Session

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 5, 2025

SUMMARY:

The Open Meetings Act permits public bodies to close their meetings to the public in circumstances outlined in §3-305 of the Act and to carry out administrative functions exempted by §3-103 of the Act. The Committee on Audit will now vote to reconvene in closed session. The agenda for the public meeting today includes a written statement with a citation of legal authority and reasons for closing the meeting and a listing of the topics to be discussed. The statement has been provided to the regents, it is posted on the USM's website and copies are available here today.

ALTERNATIVE(S): No alternative is suggested.

FISCAL IMPACT: There is no fiscal impact.

CHANCELLOR'S RECOMMENDATION:

COMMITTEE ACTION:	DATE:
BOARD ACTION:	DATE:

SUBMITTED BY: David Mosca, 443.367.0035, dmosca@usmd.edu

UNIVERSITY SYSTEM of MARYLAND

STATEMENT REGARDING CLOSING A MEETING
OF THE USM BOARD OF REGENTS

Date: June 5, 2025

Time: Approximately 11:00 AM

Location: Zoom

STATUTORY AUTHORITY TO CLOSE A SESSION

Md. Code, General Provisions Article §3-305(b):

(1) To discuss:

[ ] (i) The appointment, employment, assignment, promotion, discipline, demotion, compensation, removal, resignation, or performance evaluation of appointees, employees, or officials over whom it has jurisdiction; or

[x] (ii) Any other personnel matter that affects one or more specific individuals.

(2) [ ] To protect the privacy or reputation of individuals with respect to a matter that is not related to public business.

(3) [ ] To consider the acquisition of real property for a public purpose and matters directly related thereto.

(4) [ ] To consider a preliminary matter that concerns the proposal for a business or industrial organization to locate, expand, or remain in the State.

(5) [ ] To consider the investment of public funds.

(6) [ ] To consider the marketing of public securities.

(7) [x] To consult with counsel to obtain legal advice.

(8) [ ] To consult with staff, consultants, or other individuals about pending or potential litigation.

(9) [ ] To conduct collective bargaining negotiations or consider matters that relate to the negotiations.

(10) [ ] To discuss public security, if the public body determines that public discussions would constitute a risk to the public or public security, including:

(i) the deployment of fire and police services and staff; and

(ii) the development and implementation of emergency plans.

(11) [ ] To prepare, administer or grade a scholastic, licensing, or qualifying examination.

(12) [x] To conduct or discuss an investigative proceeding on actual or possible criminal conduct.

(13) [x] To comply with a specific constitutional, statutory, or judicially imposed requirement that prevents public disclosures about a particular proceeding or matter.

(14) [ ] Before a contract is awarded or bids are opened, to discuss a matter directly related to a negotiation strategy or the contents of a bid or proposal, if public discussion or disclosure would adversely impact the ability of the public body to participate in the competitive bidding or proposal process.

(15) [x] To discuss cybersecurity, if the public body determines that public discussion would constitute a risk to: (i) security assessments or deployments relating to information resources technology; (ii) network security information, including information that is: 1. related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity; 2. collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or 3. related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity; or (iii) deployments or implementation of security personnel, critical infrastructure, or security devices.

Md. Code, General Provisions Article §3-103(a)(1)(i):

[x] Administrative Matters

TOPICS TO BE DISCUSSED:

Discussion of personnel matters as these arise related to matters on the closed session agenda; discussion of legal matters with Counsel of the Higher Education Division of the Maryland Office of the Attorney General and receipt of legal advice; discussion of legislative audit matters that are confidential by statute as these are ongoing; discussion of investigative matters involving actual or potential criminal conduct which may lead to criminal prosecution, meeting separately with independent auditor's engagement partner and USM"s VC of accountability; discussion of IT security matters that pose

vulnerabilities of networks, critical IT infrastructure and information resources; and update of 2025 internal audit plan of activity.

REASON FOR CLOSING:

1) To maintain the confidentiality of personnel matters involved in various topics on the closed session agenda, including legal advice, investigations of possible criminal activity and ongoing legislative audits (General§3-305(b)(1))
2) To maintain confidentiality and attorney-client privilege regarding legal advice received from the OAG's Higher Education Division (§3-305(b)(7));
3) To maintain confidentiality of discussions of investigations involving possible criminal behavior, which could result in criminal prosecutions (§3-305(b)(12));
3) To maintain the confidentiality of matters involved in ongoing legislative audits, as required by Section 2-1226 of the State Government Article of the Annotated Code of Maryland (§3-305(b)(13));
4) To maintain confidentiality of USM's cybersecurity to avoid disclosing risk vulnerability of networks, critical IT infrastructure and information resources; (§3-305(b)(15);
5) To carry out an administrative function: discussion of calendar year's 2025 audit plan of activity by the USM Office of Internal Audit (§ 3-103(a)(1)(i);
7) To carry out an administrative function: the Committee's separate meeting with the VC of Accountability and independent auditors (§3-103(b)(1)(ii).