UNIVERSITY SYSTEM of MARYLAND

VIII-20.00 POLICY ON ENTERPRISE RISK MANAGEMENT

(Approved by the Board of Regents on November 22, 2019)

I. PURPOSE

Best practices in effective governance at an institution and System-wide level, requires that management periodically assesses potential risks and exposures, evaluates the probability and the impact of each and where appropriate, adopts risk mitigation strategies. These processes should inform decisions and strategic planning, both within each institution, as well as at the System level.

This policy formalizes expectations of each University System of Maryland institution to establish an ongoing system of risk management appropriate to the institution's mission and strategic initiatives. The policy also sets periodic reporting expectations and processes for reporting key risk items.

II. ENTERPRISE RISK MANAGEMENT (ERM)

A. Institution-level ERM

Pursuant to this policy, each USM institution and regional higher education center, including the USM Office, is to adopt an enterprise risk management process. The process should be developed to assure that potentially significant and likely risk exposures have been identified and communicated to institutional leadership, and that plans to reduce the risk of occurrence, or mitigate the exposure have been developed.

Under the leadership of each institution's President, an institution-wide body, such as a campus cabinet or president's leadership team, is to identify and quantify risks, determine risk tolerances, and oversee risk mitigation strategies or measures where appropriate.

The enterprise risk management process must include an inventory, or register, of risks and exposures that are potentially significant in terms of both likelihood and impact that strategic interests and goals of the institution could be impacted. Each risk should have identified a responsible official or department which will monitor and adopt mitigation strategies as appropriate, and periodically report to the institution-wide body responsible for overseeing the risk management process. Risks are to be evaluated as to the potential impact, as well as the likelihood of occurrence.

Institutions are expected to adopt risk management practices suitable and appropriate to the institution's activities and goals. Tailoring risk management activities to the institution's focus and goals may result in similar institutions assessing the likelihood, and the impact, of similarly described risks differently, with risk tolerance and mitigation

strategies that reflect those differences. Each risk management process is to include the basic steps of:

Risk identification;
Risk assessment;
Risk tolerance, prevention and mitigation; and
Reporting,

the specific risks, determination as to impact and likelihood, and accordingly, prevention and mitigation strategies, are likely to vary from institution to institution. It is important that each cycle of assessment and evaluation of risks, impact and likelihood, also consider the identification of new and emerging risks.

This policy is not intended to require a specific risk identification, assessment, mitigation or reporting process and acknowledges that institution's may have different approaches and processes to address enterprise risk management.

B. System-wide

The Chancellor is to develop a risk management process for the University System of Maryland appropriate for a comprehensive state-wide university system, that identifies, assesses, mitigates and communicates System-wide risks and exposures, and complements risk management practices at each institution. The risk assessment is to be done in consultation with the Director of Internal Audit, vice chancellors, and institution presidents, and should represent a set of identified System-wide risks and exposures appropriate to System-wide planning and action.

A review and discussion of System-wide risks and exposures, the assessment of impact and likelihood, and strategies and efforts in place to address, prevent or mitigate System-wide risks is to be considered by the Board of Regents Committee on Audits at least annually.

III. REPORTING REQUIREMENTS

Institution Presidents are expected to communicate to the Chancellor that an institutional enterprise risk management process is in place and operationally functional, and review with the Chancellor, as a part of the presidential performance review process, the 3-5 risks assessed to be the most significant concerns to institutional leadership in terms of setting strategic goals and planning.

Institution Presidents, by March 31st annually, are to provide notification to the Chancellor that a review or update of the institution's risk assessment and management plan has been performed, and are to provide a listing of significant events that have occurred in the prior calendar year that were contemplated and planned for in the institution's risk management process.

IV. DEFINITIONS

Strategic risks – an event or activity, whether internal or external, that has the potential to negatively impact the institution's ability to pursue its mission and/or achieve its key strategic goals and objectives. These risks include inadequate strategic planning and goal setting, crisis response and business continuity, reputation and brand, and community relations.

Financial risks – risks and exposures that are associated with inadequate financial planning, management and operational outcomes, including the budgeting and financial reporting processes, financial controls, debt management, endowment investing, and risk management and insurance provision.

Operational risks – risks and exposures that do not have an immediate financial impact but impact the core mission and objectives of the institution. Included here are risks to the academic enterprise such as academic quality, tenure and faculty promotion, accreditation, faculty recruitment, on-line learning, program development (including closures, new programs, and international programs). Weather events, power disruptions, and other potential events impacting availability of facilities, would be another group of operational risks, to the extent that those risks are both likely and significant in impact. Research activities and issues surrounding medical centers would also fall under the category of operational risks.

Reputational risks- risks and exposures that may harm education mission by casting doubt on commitments by campus leadership and negatively affecting the image of the University. Such risks may include claims of harassment and discrimination, waste and abuse, scholarly misconduct. Reputational risks may also be strategic, financial and operational risks depending on the nature and severity.

Risk mitigation-steps taken at the institution and System level to identify, assess and address and report on potential risks. Risk mitigation may include institution level threat and risk assessment team efforts, trainings, coordinated efforts across institutions to identify and mitigate risk.

Risk tolerance –ability or willingness by an institution or the System's leadership to accept a certain level of likelihood that a particular risk exposure materializes. Risk tolerance is important in considering the possibilities for mitigating or eliminating particular risks and exposures, each of which are likely to carry an associated cost or set of requirements.