CORPORATE POLICIES

Subject: Risk Management Policy	Policy No.: 190 Last Reviewed: March 8, 2022
Last Revision Date(s): 02/27/01, 03/08/2022	Date: September 1, 2026 Revision: 3

Purpose

This policy establishes a structured and consistent approach to risk management across Enterprises' operations. It defines how risks are identified, evaluated, managed, and monitored to support operational stability, regulatory compliance, and protection of assets. The policy supports the identification of uncertainty, reduction of potential losses, and continuity of operations. It also establishes risk management practices focused on preventing losses and supporting recovery when events occur.

Background

Enterprises maintains a conservative approach to risk management by combining preventive controls, operational practices, and transferring identifiable risks to insurers through the purchase of comprehensive insurance coverage. Enterprises operates in an environment with financial, operational, legal, and strategic risks. These risks can affect people, assets, operations, and reputation. A structured risk management program supports enterprise risk management by addressing risks across all areas of Enterprises rather than in isolated functions. This approach ensures that risks are evaluated consistently and managed in alignment with Enterprises' objectives.

Policy

I. Governance and Oversight

The Risk Management Program shall be overseen by executive leadership and administered by designated management responsible for implementation. Enterprises shall maintain an enterprise Risk Register that documents risks, assigned risk owners, existing controls, and mitigation actions. Management shall assign clear accountability for each identified risk and shall provide periodic reporting on risk exposure, mitigation progress, and emerging risks. All departments shall coordinate to support an enterprise-wide approach to risk management. Risk governance shall ensure clear authority, accountability, and alignment with Enterprises' objectives.

II. Risk Identification

Risks shall be identified on an ongoing basis and whenever significant operational, financial, or strategic changes occur. Risk identification shall include operational, financial, legal and regulatory, strategic, reputational, casualty, and event-related risks. Management shall ensure that all relevant risks are identified in a timely manner and documented appropriately to support evaluation and response.

III. Risk Evaluation and Assessment

Identified risks shall be evaluated using a consistent methodology that considers likelihood and impact. The assessment shall include quantitative analysis to estimate financial exposure and qualitative analysis to assess operational and strategic effects. Risks shall be classified according to defined levels such as high, medium, or low, and key risk drivers shall be identified. Material risks shall be defined using established thresholds and shall require active management. All evaluations shall be documented in the Risk Register.

IV. Risk Treatment Strategies

Enterprises shall determine appropriate risk responses based on evaluation results. Risk may be avoided by discontinuing high-risk activities, mitigated through the implementation of controls and process improvements, transferred through insurance or contractual arrangements, or accepted when exposure remains within approved risk tolerance. Management shall ensure that internal controls such as segregation of duties, system safeguards, and operational procedures are implemented and maintained. Insurance shall be used when risks cannot be reduced to acceptable levels through internal measures.

V. Operational Risk Management

Operational risks arising from inadequate systems, faulty controls, fraud, human error, or external events shall be actively managed. Management shall address risks related to employees, including error, misconduct, and lack of training, as well as process risks such as inadequate procedures and control failures. Management shall also address technology risks, including system failure and cybersecurity threats, and external risks such as vendor failure, fraud, and regulatory exposure. Enterprises shall implement internal controls, oversight mechanisms, and training programs to reduce operational risk.

VI. Contractual and Third- Party Risk

Contracts and agreements shall be managed to control liability and allocate risk appropriately. Enterprises shall use approved contract terms where available, verify insurance coverage from third parties, and evaluate indemnification and liability provisions. Third-party performance and compliance shall be monitored on an ongoing basis. Enterprises shall assess third-party risk prior to entering into agreements to ensure that exposures are understood and controlled.

VII. Insurance Program

Insurance shall be used as a primary method of transferring risk when appropriate. Enterprises shall maintain adequate property and casualty insurance coverage aligned with identified risk exposures and operational needs. At a minimum, Enterprises shall maintain insurance coverage in accordance with requirements established by the California State University Systemwide Office of Risk Management, including those set forth in the California State University Insurance Requirements or its successor. Coverage may include, but is not limited to, general liability, auto liability, directors and officers' liability, fiduciary liability, professional liability, employer's liability, pollution liability, workers' compensation, fidelity, and property insurance, as applicable to operations. Enterprises shall participate in the

California State University Risk Management Authority coverage program, which satisfies these insurance requirements.

VIII. Incident and Claims Management

All incidents shall be reported, documented, and managed in a timely manner. Serious incidents shall be reported immediately, and all relevant evidence and documentation shall be preserved. Enterprises shall coordinate with insurers and legal counsel as required and shall track claims and loss trends. Management shall implement corrective actions based on incident analysis to reduce the likelihood of recurrence.

IX. Monitoring and Reporting

Enterprises shall continuously monitor risks and control effectiveness. The Risk Register shall be reviewed and updated regularly, and mitigation actions shall be tracked against defined timelines. Management shall report significant risks to Leadership, the Executive Committee, or the Board of Directors, as appropriate risk tolerance and exposure levels. Enterprises shall evaluate control effectiveness on an ongoing basis, and all monitoring activities shall align with defined risk tolerance and exposure levels.

X. Review and Continuous Improvement

This policy and the risk management program shall be periodically reviewed to ensure ongoing effectiveness and risk alignment with Enterprises' operations. The review shall include periodic assessments of risks, exposures, activities, and properties, with updates made to the Risk Register and mitigation plans as needed. The policy shall also be reviewed at least every three years, or sooner if operations, regulatory requirements, or risk conditions materially change.

XI. Business Continuity and Disaster Recovery

Enterprises shall maintain business continuity and disaster recovery plans to ensure that critical operations can continue during disruptions. These plans shall include recovery procedures for systems and infrastructure, continuity procedures for essential operations, and communication protocols for emergencies. Plans shall be tested regularly and updated as necessary to ensure effectiveness.