

Enterprise Risk Management & Compliance

University Operations – Administration

EWU Policy 201-04

Effective: February 22, 2019

Authority: Board of Trustees

Proponent: Vice President for Business & Finance

Purpose: This policy describes Eastern Washington University's approach to managing risk and compliance while providing excellence in academics, student and employee opportunity and support, and community engagement. It is the policy of EWU to proactively assess and respond to any risks that may affect the achievement of EWU's mission, goals and objectives. EWU is also committed to compliance with all relevant laws, regulations and policies. EWU's commitment to managing risk and supporting compliance efforts is implemented through EWU's Enterprise Risk Management (ERM) and Compliance Program.

History: This policy supersedes EWU Policy 201-04, dated November 18, 2016. It was adopted by the Board of Trustees on February 22, 2019. Housekeeping changes were made on March 12, 2020.

Applicability: This policy pertains to all functions and operations at Eastern Washington University.

CONTENTS

- Chapter 1 – Introduction
- Chapter 2 – Risk Control and Management
- Chapter 3 – Compliance
- Chapter 4 – Responsibilities
- Appendix A – References and Related Publications

- Including risk consideration as an integral part of the decision-making process.
- Analysis of the likelihood (frequency) and impact (severity) of risks.
- Identification and prioritization of risk on an university-wide basis.
- Identification and implementation of possible risk mitigation strategies in a risk register or risk mitigation plan.

CHAPTER 1 – INTRODUCTION

1-1. General

EWU is required the university recognizes that there is exposure to risk inherent in its programs and activities. It is university policy for every employee to act to reduce risk to the greatest extent feasible, consistent with carrying out of the mission and goals of the university.

This policy provides administrative information and establishes compliance standards for enterprise risk management at Eastern Washington University.

Enterprise Risk Management is a holistic approach to risk management and encompasses risks related to all university activities including strategic, operational, compliance, financial, reputational, safety, etc. Enterprise Risk Management proactively identifies risks and opportunities across all university programs, departments or divisions. The impacts of risk or opportunities are considered not in isolation, but rather, in relation to all other agency programs and risks. This avoids departmental "silos." To achieve a mature Enterprise Risk Management program, Eastern Washington University will support and implement through its managers, supervisors and employees, coordinated Enterprise Risk Management guidelines, standards, and procedures which include, but are not limited to, the following elements:

1-2. Enterprise Risk Management Program Objectives

The university coordinates with the Department of Enterprise Services' Office of Risk Management in the development of the university's enterprise risk management program. The objectives of the Enterprise Risk Management program are to:

- promote university-wide awareness through education training and information sharing,
- allocate resources to the greatest extent feasible to services for which the state is at greatest risk of liability with the goal of preventing or mitigating loss while meeting service expectations and responsibilities,
- identify and analyze loss exposure and safety hazards,
- develop and select techniques or combinations of techniques for addressing risks,
- implement effective administration of each risk management plan, and,
- monitor the results produced or achievement of change.

1-3. Compliance Program Objectives

As a public institution of higher education, EWU is accountable for compliance with a myriad of federal and state laws and regulations. Failure to comply with these

requirements exposes the university to a variety of risks including, but not limited to, audits, inspections, fines, personal injuries, civil rights claims, lawsuits, accreditation issues, and possible loss of funding.

The purpose of EWU's compliance efforts is to proactively identify laws and regulations that impose requirements on the university and to take appropriate measures to maximize compliance with those directives.

CHAPTER 2 – RISK CONTROL AND MANAGEMENT

The university manages exposure as an inter-related risk portfolio – prioritizing loss prevention by assessing all areas of agency exposure to risk. Risk management includes actions taken both before and after a loss occurs and is directed towards reducing risks and reducing the frequency and severity of losses. When analyzing a loss exposure, the impact on the entire campus, as well as on individual departments, is evaluated.

2-1. Risk Control Methods

It is the responsibility of each unit and its personnel to conduct the business of the university in such a way as to reduce or prevent risks to the university and to evaluate the risk cost potential when determining whether to authorize new projects, activities, or programs. The University uses various combinations of the following methods to manage risks to the institution.

- a. Risk Avoidance. The university may elect to avoid undesirably high risks and programs with excessive costs by refusing to undertake unsafe activities or by discontinuing high-risk programs. In cases where the university does not have the choice to stop providing a service or program, it may be able to change how a service is delivered to avoid a risk.
- b. Accept and Monitor. This option requires the university to develop measures to track whether the risk gets better or worse over time. If the university has very low control over a risk (such as national economic conditions or natural disasters), this can be the best treatment choice.
- c. Reduce the Likelihood. Treatment should focus on making it less likely that the risk will happen by reducing the conditions that cause the risk (such as deicing a sidewalk), imposing rules to control behaviors (such as prohibiting alcohol consumption), or limiting the amount of exposure to the risk (such as limiting the amount of time a person may be exposed to potentially harmful vapors).
- d. Reduce the Impact. This option aims to reduce the impact an adverse event would have on the university's ability to achieve its goals. This can be achieved by planning for various contingencies or isolating potential risks. If the goal, for example, is to keep all university confidential information secure, then requiring password encryption of confidential information on all laptops will lessen the impact on the goal if a laptop is lost or stolen.
- e. Risk Transfer. Risk can be transferred either through an insurance policy or a contract that requires another entity to assume the risk. See section 2-2.b.

2-2. Risk Financing Methods

- a. Risk Retention. The University often retains financial responsibility for its risks of accidental loss to the maximum extent possible without jeopardizing the financial position of the University or the continuation of essential programs. Risks may be retained through either pre-funded (self-insurance) or post-funded (noninsurance) programs, after evaluation of the risk exposure. Self-insured programs are funded through contributions to the Self-Insurance Liability Fund managed by the Department of Enterprise Services, Office of Risk Management. See RCW 4.92 et. seq. and RCW 43.19 et. seq.
- b. Risk Transfer. The financial responsibility for risks may be transferred to others through contractual agreements or through the purchase of insurance. Risk can be transferred contractually through a variety of mechanisms. For example, a person seeking to participate in an event on campus may be required to sign a contract assuming the risks of participating in the event and releasing the university from any liability associated with the event. A contractor or vendor may be required, by contract, to assume certain risks associated with performing certain services or providing certain goods and to indemnify the university for any harm arising out of the contractor or vendor's performance. There are other contractual risk transfer mechanisms available, such as performance bonds, escrow accounts, and mandating certain types of insurance coverage. Any person entering into a contract on behalf of the university should be familiar with these risk transfer options.

Insurance is another form of transferring risk. The Risk Manager may require departments, programs, student groups, or outside entities to purchase insurance at their expense before an activity is approved. The Risk Manager may also

choose to purchase insurance on behalf of the university when it is not deemed prudent to retain the risk based on comparison of the cost of insurance with the risk potential. Further, the University may purchase insurance when required by law, bond, or contractual agreement, when real properties are financed with student fees or other non-state appropriated funds, or when non-university property is under the care, custody, or control of the University. Commercially insuring risks does not alter the responsibility of the University, its units, or personnel for compliance with required and appropriate safety/security standards.

CHAPTER 3 – COMPLIANCE MANAGEMENT

3-1. Commitment

EWU is committed to compliance with all relevant federal and state laws, regulations and policies. The university outlines the below measures to maximize compliance with those laws, regulations and policies.

3-2. Culture of Compliance

EWU integrates compliance efforts in alignment with the university's mission and values while striving to build a culture of compliance.

3-3. Compliance Program Responsibility

It is the responsibility of every employee and student to conduct the business of the university in compliance with relevant laws, regulations, and policies. The university compliance program includes the following activities:

- a. Identification. The university proactively identifies laws, regulations, and policies that govern our operations and activities.
- b. Assessment and Response. EWU assesses legal requirements and determines how best to maximize university-wide compliance with those requirements. University compliance efforts typically include compliance assessments, identification of responsibilities, policy making, alignment with existing policies and practices, communications, training, reporting, response, and ongoing monitoring.

CHAPTER 4 – RESPONSIBILITIES

4-1. Board of Trustees

The EWU Board of Trustees has a fiduciary duty to exercise careful, prudent oversight in a manner consistent with EWU's mission and best interests. In

relation to enterprise risk management and compliance, the Board of Trustees:

- approves the overall enterprise risk management and compliance structure;
- ensures the ERM and compliance program is independent, respected, and appropriately resourced;
- receives quarterly updates and an annual ERM and compliance report; and,
- provides executive level feedback to guide risk and compliance efforts.

4-2. President, Provost & Vice President for Business & Finance

The President, Provost, & Vice President for Business & Finance share the Board's responsibility for governance of the university; set the tone and example for the university community about the importance of ERM and risk management; and, are responsible for making decisions pertaining to any significant risk or compliance issues. The President, Provost and Vice President for Business and Finance:

- receive regular updates from the ERM and compliance workgroup;
- prioritize risk and compliance activities and direct relevant resources accordingly; and,
- make decisions regarding circumstances that present a significant risk or compliance concern.

4-3. Associate Vice President for Civil Rights, Compliance & Enterprise Risk Management

The Associate Vice President for Civil Rights, Compliance & Enterprise Risk Management is responsible for directing and coordinating university-wide ERM and compliance endeavors and communicating matters of significant risk to the President, Provost, or Vice President for Business and Finance. The AVP chairs the ERM and compliance workgroup; regularly reports to the President, Provost, or Vice President; provides a quarterly and annual report to the Board of Trustees; and oversees the development of university policies.

4-4. Director of Risk Management

The Director of Risk Management provides technical support to university ERM activities including risk identification, assessment and mitigation. The director reviews requests for campus activities; coordinates identification and procurement of institutional insurance; prepares releases and waivers for institutional activities; and assists in coordination of ERM activities and development of ERM communication and training materials.

4-5. ERM and Compliance Work Group

The ERM and Compliance Work Group is charged with identifying ERM and compliance goals and priorities, monitoring regulatory changes, establishing projects to

address compliance goals, and leveraging resources for greater efficiency and effectiveness. The ERM and Compliance Work Group:

- prioritizes risks identified in the development of the university's risk register;
- identifies areas where there are significant risk and compliance concerns;
- develops work plans to mitigate risk and/or improve compliance in relevant areas;
- monitors risk mitigation efforts; and,
- receives reports of any significant risk or compliance concerns.

The ERM and Compliance Work Group includes subcommittees that are charged with identifying risk and compliance concerns; implementing risk mitigation measures; and identifying and operationalizing improved compliance efforts.

The ERM and Compliance Work Group is chaired by the AVP for Civil Rights, Compliance, and Enterprise Risk Management and includes designated university staff members with responsibilities for:

- health & safety;
- research & intellectual property;
- employment & civil rights;
- information security;
- financial operations;
- institution reputation; and,
- competitive position.

4-6. University Leaders & Managers

Leaders have a significant role to play in the risk management and compliance efforts of the university. They set the tone and influence the culture of risk management and compliance by:

- Determining risk tolerance, that is whether the agency is 'risk taking' or 'risk averse' as a whole, or on any specific issue;
- Determining which risks are acceptable and which are not;
- Setting standards and expectations of staff with respect to conduct, risk inquiry, and compliance;
- Monitoring the management of mission-critical risks;
- Satisfying itself that the less mission-critical risks are also being actively managed by staff who are risk owners and that there are appropriate and effective controls in place; and
- Reviewing annually the agency's approach to risk management, losses in the previous year, and approving changes or improvements to key elements of risk assessment processes and procedures.

4-7. Department Head/Chair Responsibilities

Department heads/chairs are responsible for managing risk and maximizing compliance within their departments. They must be knowledgeable about the university's

Enterprise Risk Management and Compliance policy and related guidelines.

Department heads/chairs shall:

- Identify and take steps to involve employees, students, and community members served by the university in efforts to lessen the risk associated with university activities and services.
- Share risk management and compliance guidance and standards with employees, students, and affiliated groups.
- Ensure departmental activities, travel, events, field trips, etc. are subjected to an appropriate risk assessment and comply with all applicable laws and policies.

4-8. Event/Activity Sponsors

Sponsors of university events or activities must be knowledgeable about the university's Enterprise Risk Management and Compliance policy and related guidelines.

Sponsors must ensure that all steps have been followed and the appropriate risk assessment forms have been completed for their event/activity, to include a review by the university Risk Manager and final approval prior to the event and/or activity. If the requestor of an event/activity chooses not to follow the recommendation of the Risk Manager, they may request a waiver from their vice president or the university president if applicable.

4-9. Employees

Eastern Washington University employees are encouraged to support the university's efforts to identify, eliminate or manage risk and compliance efforts across all divisions, offices and functions. Offices must work together across boundaries to share internal control methods and procedures that implement a comprehensive and coordinated set of processes and approaches to Enterprise Risk Management and Compliance.

APPENDIX A – REFERENCES AND RELATED PUBLICATIONS

- RCW 43.19.760 – Risk Management Principles
- RCW 43.19.763 – Risk Management – Definitions
- Governor’s Executive Order 16-06 State Agency Enterprise Risk Management
- SAAM 20.20 Risk Assessment
- EWU Policy 203-01, Information Security
- EWU Policy 203-02, Copyright Infringement
- EWU Policy 401-06, Protected Health Information
- EWU Policy 201-02, Preservation of Electronic Records
- EWU Policy 204-03, Access Control
- EWU Policy 603-03, Fire Safety
- EWU Policy 603-01, Campus Safety, Security and Crime Prevention
- WAC 172-64, Alcohol Policy at EWU