ENTERPRISE RISK MANAGEMENT POLICY

Policy Authority: Vice-President, Finance and Administration (“VPFA”)

Associated Procedure(s): Enterprise Risk Management Procedures (“ERM Procedures”)

EXECUTIVE SUMMARY

The University takes on risk as a necessary part of its operation. This policy sets out the principles the University will follow and the activities it will undertake for effectively managing institutional risks, and establishes roles, responsibilities, and accountabilities for Enterprise Risk Management (“ERM”).

The University has a program of risk identification, mitigation, and transfer across six categories of risk; compliance, environmental, financial, operational, reputational, and strategic. This program is reviewed regularly and is informed by both provincial and internationally accepted risk management standards and guidelines.

The risk management procedures followed by the University and the results are documented. The University Executive formally assesses the management of institutional risks, including key emerging risks, on at least a semi-annual basis and provides a report to the Board of Governors.

TABLE OF CONTENTS

1.0 PREAMBLE ........................................................................................................ 2
2.0 PURPOSE .......................................................................................................... 2
3.0 SCOPE AND JURISDICTION ............................................................................ 2
4.0 DEFINITIONS ..................................................................................................... 2
5.0 POLICY ............................................................................................................ 2
6.0 ROLES AND RESPONSIBILITIES ................................................................. 3
7.0 REPORTING ...................................................................................................... 4
8.0 RELATED LEGAL, POLICY AUTHORITIES AND AGREEMENTS .......... 4
9.0 ACCESS TO INFORMATION AND PROTECTION OF PRIVACY .............. 4
10.0 RETENTION AND DISPOSAL OF RECORDS ................................................. 4
11.0 POLICY REVIEW ......................................................................................... 5
12.0 POLICY AUTHORITY .................................................................................... 5
13.0 INTERPRETATION .......................................................................................... 5
14.0 PROCEDURES AND OTHER ASSOCIATED DOCUMENTS ..................... 5
1.0 PREAMBLE

1.1 Simon Fraser University ("the University") is committed to implementing and maintaining a sustainable Enterprise Risk Management ("ERM") process across the institution. The University recognizes that in undertaking activities not all risk can, or should be, eliminated. Although risk management often involves responding to the negative impacts of risk, all opportunities bring some risk which must be effectively managed, and not necessarily avoided. Awareness and management of risks is critical for protecting the University.

Every member of the university community has a role to play in risk management and is expected to adopt strategies that balance risks and rewards when undertaking activities on behalf of the University.

The University supports ERM through an active program of risk identification, mitigation, and transfer across six categories of risk: compliance, environmental, financial, operational, reputational, and strategic. The University reviews the approach to ERM regularly to ensure the timely implementation of best practice based on provincial risk management guidelines as well as internationally accepted risk management standards.

2.0 PURPOSE

2.1 This policy sets out the principles the University will follow and the activities it will undertake in managing institutional risks, and establishes roles, responsibilities, and accountabilities for ERM.

2.2 This policy is intended to provide a consistent foundation for risk management. The policy is supported by the ERM Procedures which will be updated as needed to reflect changes in the University’s practices, stakeholder expectations, as well as SFU’s strategic plan and objectives.

3.0 SCOPE AND JURISDICTION

3.1 This policy applies to all members of the university community and to all university activities, whether in Canada or abroad.

4.0 DEFINITIONS

4.1 Please see Appendix A for the definitions of words used in this policy and its associated procedures.

5.0 POLICY

5.1 The implementation and continuous improvement of Enterprise Risk Management will be guided by the following principles:

5.1.1 The University takes on risk as a necessary part of its operation and acknowledges that all activities have an element of risk and that not all risks can be fully mitigated or transferred. Effective risk management is an essential aspect of operating the University.
5.1.2 The University manages risks through an integrated and systematic approach to ensure structured and consistent consideration of risks in key decision-making.

5.1.3 The University manages its risks in order to minimize risk and optimize reward, in a manner that balances the cost of managing risk with the anticipated benefit(s).

5.1.4 ERM is a shared responsibility at all levels of the university, from the Board of Governors to individuals. Employees are expected to understand the risks that fall within their area of responsibility and are expected to manage these risks.

5.1.5 The ERM Procedure under this policy will outline Enterprise Risk Management processes and activities and will continuously evolve to reflect external and internal conditions and to align with the University’s strategic plan, institutional goals, and operational requirements.

5.2 The University will establish, implement, and conduct the following activities to facilitate effective risk management and reporting:

5.2.1 Use the ERM Procedures to apply ERM consistently across all major processes to ensure structured and consistent consideration of risks in key decision-making.

5.2.2 Perform continuous risk monitoring and conduct a formal risk assessment semi-annually to update the University’s risk profile with respect to existing and emerging risks, and report findings to the Board of Governors.

5.2.3 Report current status and risk strategies to the Board of Governors at a minimum, on a semiannual basis.

5.2.4 Align ERM objectives and procedures with other internal risk programs to ensure effectiveness and efficiency.

5.2.5 Conduct ongoing ERM program to identify opportunities for improvement in response to changing internal or external conditions.

6.0 ROLES AND RESPONSIBILITIES

6.1 The following are responsible for ERM activities:

6.1.1 Board of Governors (“Board”): The Board has ultimate oversight of, and responsibility for, the University’s risk management structures and processes. The Board, through its Audit, Risk and Compliance Committee (“ARCC”) reviews semi-annual ERM reporting.

6.1.2 University Executive: University Executive is accountable for the risk management activities of the University. They review and approve changes to the Risk Register, perform the assessment of risks and approve semi-annual ERM reporting. The University Executive may delegate monitoring, managing, and mitigating risks through the assignment of Executive Risk Leads.
6.1.3 **Vice President, Finance and Administration** (“VPFA”): The VPFA oversees the development of the ERM Policy and the ERM Procedure as well as the overall operation of Enterprise Risk Management.

6.1.4 **Executive Risk Lead** (“ERL”): The Executive Risk Lead is responsible for monitoring, responding to, and reporting on the institutional risk to which they have been assigned, and to ensure that individual employees understand and manage the risks that fall within their area of responsibility.

6.1.5 **Safety and Risk Services**: Safety and Risk Service is responsible for the development and facilitation of Enterprise Risk Management and facilitating risk management reporting for the University.

6.1.6 **Internal Audit**: Internal Audit is responsible for providing independent and objective assurance on the University’s risk management and internal control framework to the Board.

### 7.0 REPORTING

7.1 The risk management procedures followed by the University and the results must be supported by appropriate records and documentation. The University Executive will formally assess the management of risks, including identification of key emerging risks, on at least a semi-annual basis and submit formal reports to the Board.

### 8.0 RELATED LEGAL, POLICY AUTHORITIES AND AGREEMENTS

8.1 The legal and other University Policy authorities and agreements that may bear on the administration of this policy and may be consulted as needed include but are not limited to:

8.1.1 *University Act*, R.S.B.C. 1996, c. 468


### 9.0 ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

9.1 The information and records made and received to administer this policy are subject to the access to information and protection of privacy provisions of British Columbia’s *Freedom of Information and Protection of Privacy Act* and the University’s Information Policy series.

### 10.0 RETENTION AND DISPOSAL OF RECORDS

10.1 Information and records made and received to administer this policy are evidence of the University’s actions to identify, measure, assess, respond to, monitor, and report on risks that affect the achievement of the University’s strategic plan or institutional goals. Information and
records must be retained and disposed of in accordance with a records retention schedule approved by the University Archivist.

11.0 POLICY REVIEW

11.1 The Vice President Finance and Administration will undertake a systematic approach to monitoring and evaluating this policy and its associated procedures and practices to ensure that they are responsive to evolving needs and the evolving environment. This includes but is not limited to:

11.1.1 Reporting semi-annually to the Board on the implementation of the policy;
11.1.2 Periodic reviews of the University’s training and educational initiatives related to ERM; and
11.1.3 Reviewing this policy at least every three years.

12.0 POLICY AUTHORITY

12.1 This policy is administered under the authority of the Vice President Finance and Administration.

13.0 INTERPRETATION

13.1 Questions of interpretation or application of this policy or its procedures shall be referred to the Vice President, Finance and Administration, whose decision shall be final.

14.0 PROCEDURES AND OTHER ASSOCIATED DOCUMENTS

14.1 Appendix A contains the definitions applicable to this policy and its associated procedures.
14.2 The procedures for this policy are: Enterprise Risk Management Procedures.