DAWSON COLLEGE

No. BOG-DG-05

Title: RISK MANAGEMENT POLICY

CLASSIFICATION: DIRECTOR GENERAL
FIRST ADOPTED: September 24, 2019

Article 1 Objectives

This policy defines a systematic approach to manage the risks that could affect the College. It aims to support risk-informed decision making: to foster a culture that is risk-aware without being risk-averse, pursuing opportunities that further strategic and operational priorities, while effectively managing risk.

Article 2 Legal Context

This policy is applied in accordance to applicable laws, bylaws, regulations and policies, including but not limited to:

- the *Act respecting contracting by public bodies* (CQLR C-65.1) and the *Directive concernant la Gestion des Risques en Matière de Corruption et de Collusion dans les Processus de Gestion Contractuelle, Secrétariat du Conseil du Trésor,* hereafter the *Directive on Contract Management*
- the *Act Respecting the Governance and Management of Information Resources (CQLR, G-1.03),* hereafter *the IT Governance Act,* and the *Directive sur la sécurité de l'information gouvernementale, Secrétariat du Conseil du Trésor,* hereafter *the Directive on Information Security*

Article 3 Risk Management Process

The College methodology for risk management is based on the process described in the International ISO 31000 and Australian APES 325 standards for risk management.

Representatives from various areas of expertise are brought together throughout the process, to ensure different views are considered when defining criteria, evaluating risk, and to build a sense of ownership among those affected by risk. For example, risks related to corruption and collusion might involve representatives from financial services, purchasing department, contractual rules compliance, etc.

3.1 Establishing the context

The context defines:

- the scope of the process, i.e. the timeframe, depth of the analysis, and resources required
- the external factors, which could be for example: demographics, regulatory and budgetary framework, relationships with partners, etc.
- the internal factors, i.e.: who are the stakeholders, what are the relevant relationships and dependencies within the organisation, what are the objectives and strategies
- the evaluation criteria which determines the level of risk the College is prepared to accept

3.2 Risk identification

The identification consists of recognising and describing the event, its possible causes and consequences. An example of risk could be the disclosure of sensitive information. It could be

caused by inappropriate information security measures. Consequences could be release in the press or ministerial intervention.

3.3 Analysis and evaluation

The analysis determines the likelihood of a risk occurring and the impact it would have should it occur. The likelihood is a subjective ranking rather than a mathematical certainty. Examples of a rare likelihood could be an event with less than 5% chance of occurring, or an once every five years. Examples of major impact could be significant financial loss, extended disruption of services, damage to the College reputation, etc.

The purpose of the evaluation is to determine the overall significance of a risk, based on its likelihood and impact. A low likelihood and low-impact risk is deemed the less significant, and high likelihood and high-impact are deemed the most significant.

3.4 Risk treatment

The treatment of a risk is the selection of the most appropriate option and the elaboration of an action plan. The option might be:

- to avoid the risk, by selecting an alternative rather than proceeding with the activity
- to mitigate the risk, by introducing a strategy designed to reduce the likelihood or the impact
- to monitor the risk, when there is uncertainty with the likelihood or concerns with its evolution.
- to accept the risk, is to make an informed decision that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit

3.5 Monitoring and review

The identified risks must be regularly re-evaluated and the incidents or 'near-miss' logged. The action plan needs to be evaluated, and the outcomes measured. The efficiency of the risk management process must also be evaluated and reviewed.

Article 4 Regulatory Framework

The College is subject to specific requirements, stated in the Directive on Contract Management and the Directive on Information Security.

4.1 Risks of corruption and collusion in contract management

The Directive on Contract Management establishes requirements for a risk management framework with regards to corruption and collusion, an annual plan and a review report.

4.1.1 Annual plan

Every financial year an annual plan must be adopted. The plan includes:

- An analysis of the context for contract management
- The assessment of risks, including identification, analysis and evaluation
- The measures for treatment of risks
- Any other element determined by the Treasury Board.

4.1.2 Review report

Each annual plan is subject to a review report, which must be adopted no later than four (4) months after the end of the financial year. The report includes:

- A measure of the outcomes for risk management
- A measure of progress and differences ('ecarts') with the previous plan

- Results of the verification of efficiency of the risk management framework
- The review of the risk management framework
- Any other element determined by the Treasury Board

4.2 Information security risks

The Directive on Information Security requires the College to adopt a formal process for risk management, and to declare risks to the *Dirigeant Principal de l'Information* nominated by the Ministry.

Article 5 Roles and Responsibilities

5.1 Board of Governors

The Board of Governors adopts this policy, and delegates to the Director General other responsibilities stated in the Directive on Contract Management.

5.2 Director General

The Director General :

- Is responsible for the application of this policy
- Adopts the annual plan and the review report for risk management of corruption and collusion in contract management
- Within fifteen (15) days of a request by the President of the Treasury Board, provide the annual plans and review reports, as well as related documentation,
- Reports to the Board of Governors on the application of this policy
- Recommends amendments to this policy to the Board of Governors

Article 6 Final Provisions

This policy is effective on the date of adoption.