Summary
Information Security Policy

This document is a summary (the "**Summary**") of Laurentian Bank of Canada Financial Group's ("**LBCFG**") Information Security Policy (the "**Policy**"). Since the Policy is reviewed and amended from time to time, this Summary may not fully reflect the up-to-date version of the Policy. In the event of a conflict between the content of this Summary and the provisions of the Policy, the Policy shall prevail.

1. PURPOSE AND SCOPE

The Policy is part of the information security program of LBCFG. It encompasses all aspects of information security surrounding LBCFG, including information security requirements and LBCFG's commitment to protect its employees, contractors, clients, and information utilized to attain its business goals. Thus, the main objectives of the Policy include the following:

- Maintaining the confidentiality, integrity and availability of information;
- Ensuring awareness and compliance by all users with all current and relevant legislation in connection with the confidentiality, integrity, and handling of LBCFG's information;
- Providing principles by which a safe and secure working environment can be established;
- Protecting LBCFG from liability or damage from the misuse of its information technology facilities; and
- Maintaining all data and information at a level of security consistent with its classification, including upholding any legal and contractual requirements around information security.

The Policy applies to all lines of business and sectors of LBCFG and must be adhered to by all users that access, process, use, maintain or handle LBCFG's information throughout its lifecycle, including LBCFG's employees, contractors, vendors and third party suppliers. It covers LBCFG's information in any form, whether physical or digital, regardless of where it resides, where it is stored or processed, or who is responsible for its processing or storing.

2. CONTENT

The Policy describes LBCFG's information security program and some of its related guidelines and procedures, which apply in accordance with business requirements and relevant laws and regulations. Topics covered in the Policy include the following:

- Access to data, information, systems, applications, networks and premises;
- User registration, deregistration, authentication and access rights;
- Classification, labelling and handling of data;
- Responsibility, inventory, ownership, acceptable use and return of assets;
- Protection of assets against loss, damage, theft or compromise;
- Protection of information by cryptographic means;
- Data and information back-up processes;
- Logging and monitoring of the activity on LBCFG's networks;
- Detection, prevention, and recovery controls to protect against malware and spam;
- Secure operation of information processing facilities;
- Installation and restriction of software installations;

- Prevention of the exploitation of technical vulnerabilities in LBCFG's systems and protection of the supporting infrastructure;
- Network segregation and related security measures;
- Information transfer procedures;
- Information security training and awareness initiatives;
- Security measures in connection with the use of mobile devices and remote access;
- Security measures in connection with the end of a business or employment relationship;
- Monitoring and review of suppliers and third parties to ensure information security compliance;
- Integration of security controls, service definitions and delivery levels in third-party service delivery agreements;
- Information security incident reporting, management and improvements;
- Information security continuity and related business continuity plans;
- Compliance with legal, statutory, regulatory and contractual obligations;
- Cyber risk assessment, testing and mitigation;
- Contact with relevant authorities, special interest groups or other specialist security forums and professional associations; and
- Independent reviews of information security.

The Policy also details the roles and responsibilities of management, the board of directors, as well as various groups, committees and individuals, within and outside of LBCFG, in applying the Policy and the guidelines and procedures adopted under LBCFG's information security program.

3. ENFORCEMENT

Compliance with the Policy and its supporting guidelines is mandatory and binding for LBCFG's employees, contractors, vendors and third party suppliers. Failure to comply with the intent of the Policy may result in actions by LBCFG which include denial of access to LBCFG's information and systems, disciplinary or contractual action such as written warnings, suspensions with or without pay and/or immediate dismissal or termination of agreement, and civil or criminal prosecution.

4. REVIEW

The Policy is reviewed at least annually by LBCFG's IT Governance Department and the Chief Information Officer. It is then submitted to the board of directors of LBCFG for its approval. Directives and procedures adopted under the Policy are reviewed at least every two (2) and three (3) years, respectively.

October 2021