



FingerMotion

FINGERMOTION, INC.
(the “Corporation”)

RISK AND INFORMATION SECURITY COMMITTEE CHARTER

Purpose

The Risk and Information Security Committee (the “Committee”) assists the Board of Directors of FingerMotion, Inc. (the “Corporation”) by overseeing and reviewing:

- a. Internal controls to protect information and proprietary assets; and
- b. Risk governance, including the Enterprise Risk Management framework, risk policies, and risk tolerances.

The Committee collaborates with the Audit Committee to ensure related matters are appropriately addressed.

Responsibilities

The Committee's key duties include:

- a. Setting the tone for information security and enterprise risk management;
- b. Ensuring alignment between the Corporation's information security and risk management strategies and objectives;
- c. Independently reviewing the Corporation's information security framework and risk management system; and
- d. Evaluating the risk governance structure, including the enterprise risk management framework, key risk policies, and critical risk tolerances.

The Committee is empowered to investigate any matter, access all relevant records and personnel, and retain independent consultants at the Corporation's expense. The Corporation will provide funding for such activities as necessary.

Scope

This Charter applies to FingerMotion, Inc. and its subsidiaries in the U.S. and abroad.

Membership

The Board of Directors appoints Committee members, who should have relevant experience in areas such as:

- a. Familiarity with major technology platforms used by the Corporation.
- b. Knowledge of technological ecosystems and business environment challenges.
- c. Understanding of emerging technologies and cybersecurity threats.
- d. Experience with enterprise risk management principles and processes.
- e. Meetings

The Committee meets as needed and may require attendance from any Corporation officer, employee, or consultant. Regular executive sessions will be held for private discussions. Minutes will be recorded for each meeting.

Roles & Responsibilities

Management is responsible for maintaining a robust information security system and managing the risk function. The Committee oversees these activities, relying on information and representations from management. The Chief Financial Officer and the lead information technology manager (the "IT Manager") of the Company's contractually controlled subsidiary, Shanghai JiuGe Information Technology Co., Ltd., report directly to the Committee.

Specific duties include:

- a. Reviewing information security and cyber threat policies with the IT Manager and management;
- b. Assessing frameworks to prevent, detect, and respond to cyber attacks, and identifying vulnerabilities;
- c. Evaluating policies and frameworks for access controls, incident response, business continuity, disaster recovery, and IT asset protection;
- d. Reviewing employee education programs on information security issues;
- e. Receiving reports on assessments from the IT Manager and other departments;
- f. Approving the risk governance structure, enterprise risk management framework, key risk policies, and critical risk tolerances;
- g. Discussing major risk exposures with management and the Chief Financial Officer;

- h. Approving the internal audit work plan;
- i. Receiving reports on risk management reviews and assessments from relevant departments;
- j. Reporting regularly to the Board of Directors and reviewing significant issues;
- k. Making recommendations to the Board as necessary;
- l. Annually reviewing and updating the Committee's Charter; and
- m. Performing other duties as needed.

Reports

The Committee will document its recommendations to the Board in written summaries, included in the minutes of the Board meeting where presented.

Minutes

The Committee will maintain written minutes of its meetings, filed with the Board meeting minutes.