FINGERMOTION, INC.
(the "**Corporation**")

CYBERSECURITY POLICY

Purpose

The purpose of this Cybersecurity Policy (or the "**Policy**" as the context provides for) is to serve as a standard for protecting the organization against cybersecurity threats.

The information that exists within the information technology ("**IT**") network and infrastructure (the "**Cyberspace**") is a valuable asset of the Corporation and, therefore, benefits from protection and preservation thereof. Effective information security management is necessary for the secured sharing and protection of information within the Corporation's Cyberspace.

This Policy serves as a framework that all employees, directors and officers shall abide by to ensure that risks to the confidentiality, integrity or availability of the Corporation's assets within the Cyberspace are managed in accordance with the agreed upon cybersecurity approach.

Applicability

This Policy applies to all directors, officers, employees, agents and contractors of the Corporation and any parent, holding companies and subsidiaries regardless of the terms of their contract (collectively, "**you**"), who use the Corporation's technological devices or otherwise access information within the Corporation's Cyberspace. References in this Policy to "**we**", "**us**" or "**our**" shall be interpreted as referring to the Corporation unless the context suggests otherwise.

Policy Statement

The Corporation recognizes the importance of effective information security management and strives to maintain the confidentiality, integrity and availability of information in the Cyberspace. In aspiring to prevent, detect and respond to unauthorized and malicious attacks in the Cyberspace, the Corporation will identify, prioritize and manage dedicated efforts towards both protection of information and the minimization of risks of unauthorized and malicious access to information in the Cyberspace.

The Board of Directors of the Corporation (the "**Board of Directors)** aims to lead the Corporation in a direction that minimizes the risk of unauthorized and malicious use, disclosure, potential theft, alteration, or damaging effects of the Corporation's operations while concurrently enabling the sharing of information in the Cyberspace. The Board of Directors is committed to ensuring that risks to the confidentiality, integrity or availability of Corporation-owned information assets are

managed and appropriately mitigated by implementing an information security risk management approach. In furthering the Corporation's mission to protect information within the Cyberspace as a valuable asset, the Corporation is committed to its information security program aimed at securing the information asset of the organization. In addition, the Corporation strives to ensure continued protection and maintenance of a secure environment for users of its Cyberspace information by aligning its information security approach. This includes reserving a right to monitor and audit network and system usage at any time for compliance reasons pursuant to this Policy. The Corporation views all reports of breaches hereunder seriously and will abide by rigorous investigation processes in the event of a breach.

Material Incidents

Team leads from various departments of the Corporation will report to the Corporation's Chief Financial Officer (the "**CFO**") with regard to any violations of this Policy or other cybersecurity incidents.

The CFO will lead the review of all reported cybersecurity incidents to determine if they materially affect the organization. If determined to be material, the Risk and Information Security Committee (the "**RIS Committee**") and Board of Directors should be notified immediately, and an Item 1.05 Form 8-K must be filed within 4 business days describing the following:

- Material aspects of the nature, scope, and timing of the incident
- Material impact or reasonably likely material impact of the incident on the organization, including its financial condition and results of operations

Risk Management

Risk Assessment

The Corporation will conduct an annual cybersecurity risk assessment as part of the overall risk management process. The purpose of this assessment includes the following:

- Identify cybersecurity risks relevant to the organization, including those associated with processes performed by third-party service providers
- Assess the organization's current processes and controls to determine the effectiveness of ongoing risk management and mitigation
- Recommend enhancements as needed to better equip the organization in mitigating cybersecurity risks
- Determine if any risks, including as a result of previous incidents, have materially affected or are reasonably likely to materially affect the organization
- Develop remediation plans as needed to enhance processes and controls, prioritizing those with material impact to the organization

The CFO is responsible for ensuring the risk assessment is completed by a team with expertise in cybersecurity risk, whether it is performed internally or through the use of a third party.

The Corporation will engage a third-party(ies) in connection with the annual risk management process.

Oversight

The RIS Committee of the Corporation will oversee this policy and will be responsible for the implementation of the Corporation's oversight, programs, procedures, and policies related to cybersecurity, cybersecurity risks, information security, and data privacy.

Management shall report to the RIS Committee on the Corporation's and its subsidiaries' strategy, risks, metrics and operations relating to cybersecurity and information security matters. This includes results of the cybersecurity risk assessment and related remediation plans, cybersecurity incidents, significant cybersecurity and information security-related projects and initiatives and related progress, the integration and alignment of such strategy with the Corporation's overall business and strategy, and trends that may affect such strategy or operations.

The RIS Committee shall report at least annually to the Board concerning matters covered under this Policy and advise the Board of any developments that the Committee believes should have Board consideration. The RIS Committee shall also review and assess the adequacy of this Policy at least annually and recommend any proposed changes to the Board for approval.

Disclosure

The annual Form 10-K requires disclosure of the organization's cybersecurity risk management process for material risks as well as the role of management and the Board of Directors in the assessment, management, and oversight of these risks.

Employee Responsibility

All employees shall exercise professional judgement in using computing devices and network resources connected to the Cyberspace. All information, including physical and intellectual properties stored on electric and computing devices or existing within the Cyberspace remain the sole property of the Corporation. Therefore, employees must neither access nor share confidential and proprietary information prior to receiving consent from management or the Corporation's directors and officers.

Employees are strictly prohibited from performing any act that would be contrary to this Policy, including but not limited to:

- accessing Corporation data, a server or an account for any purpose other than conducting the Corporation's business in ordinary course;
- copying or distributing copyrighted material or intellectual property without prior consent;

- installing any copyrighted software without obtaining approval from the Corporation's third party IT group;
- sharing passwords with other individuals or allowing others access to your accounts;
- exporting software, technical information, encryption software or technologies prior to obtaining consent from either management or the Corporation's third party IT group; and
- making fraudulent offers of products, items or services from any account that represents the Corporation.

All potential threats or loss of any Corporation device that may store confidential information must be promptly reported to the CFO.

Management Responsibilities

First and foremost, the Corporation's management team shall facilitate an environment whereby managing cybersecurity risk is accepted as the personal responsibility of each member of the Corporation.

Management will ensure that employees are provided with adequate resources to fully understand the guidelines and expectations for cybersecurity. Members of the management team may be asked by the CFO to assist with IT security investigations in the event of a breach of this Policy. Upon becoming aware of a potential violation of this Policy or a breach of cybersecurity, the member of management must immediately document the violation and request the individual surrender possession of any devices that may have suffered a security breach.

Regulatory Developments

The RIS Committee shall monitor, on an ongoing basis, the implementation and effectiveness of this Policy and shall, annually or more frequently when applicable, assess:

- key legislative and regulatory developments that could materially impact the Corporation's cybersecurity and digital technology strategy, operations or risk exposure;
- engagement with government agencies, industry peers, and other critical infrastructure sectors on cybersecurity and related resiliency;
- industry trends, benchmarking and best practices relating to cybersecurity and digital technology; and
- any relevant cybersecurity and digital technology metrics.

Restrictions and Limitations

Individuals who are subject to this Policy are not limited to the restricted use of specific devices. This Policy is all encompassing and incorporates all future and personal devices that may be used to store IT and confidential information of the Corporation, including intellectual property.

Enforcement

Failure to comply with this Policy or support this Policy and the mandates herein may compromise the Corporation's information assets and cause irreparable harm to the organization, its people, clients and digital and physical assets. For further clarity, violations of this Policy may include, but are not limited to, the conscious release of data or confidential information to unauthorized parties, conscious downloads of software or hardware that jeopardizes the security of the Corporation, and openly sharing passwords with any individual. Violations of this Policy or the associated schedules, standards or guidelines may result in suspension, discipline up to and including termination, in addition to administrative sanctions or legal actions.

.