Get More Math Information Security Policy

Document Type:	Company Policy
Version:	7.0
Date of version:	3/25/2024
Created by:	Ben Norman
Approved by:	Josh Britton
Confidentiality level:	Public

Table of contents

1. PURPOSE 2
2. INTRODUCTION 2
3. SCOPE 2
4. GOALS 3
5. POLICY STATEMENTS 3
6. RESPONSIBILITIES 3
7. DOCUMENT MANAGEMENT, CONTINUAL IMPROVEMENT 4
8. CHANGE HISTORY 4

1. Purpose

This document defines Get More Math's policy on Information Security and is based on the following principles. (Get More Math is also referred to as "The Company" in this document).

- Maintaining confidentiality, integrity and availability of information.
- Handling information appropriately and according to its data classification.
- Preventing service disruptions that lead to financial loss or loss of reputation to the Company.
- Ensuring business continuity and minimizing business damage by managing and minimizing the impact of information security events.

2. Introduction

The confidentiality, integrity and availability of information are of great importance to the operation and administration of Get More Math. Failure in any of these areas can result in disruption to the services that the Company provides, as well as a loss of confidence in the Company by existing and potential clients. The security of our information and assets is therefore regarded as fundamental to the successful operation of the Company.

3. Scope

This policy applies to:

- All Company staff and contractors
- All information assets owned or managed by the Company
- Access rights and controls to information
- Security of services and information systems
- Business continuity and disaster recovery of information
- Appropriate controls to meet regulatory and legislative requirements
- Framework for third parties and Company staff to adhere to
- Promotion of security, guidance and advice where appropriate
- Processes to deal with security breaches

4. Goals

Get More Math's Information Security policies should provide business continuity and minimize business damage by preventing and managing to an acceptable level the impact of information security incidents. Additionally, these policies should provide a framework to ensure that GMM team members understand the company's commitment to information security, their roles and responsibilities in maintaining a secure and functional application, and procedures and escalation paths for security events.

Adherence to these policies will help to protect the Company, our clients, and staff from information security threats, whether internal or external, deliberate or accidental.

5. Policy Statements

These policy objectives are achieved through the implementation of our Information Security Management System, which includes security standards, procedures and guidelines developed with the goal of maintaining alignment with the NIST Cybersecurity Framework. It is the Company's policy to meet all information security requirements under appropriate regulation, legislation, organizational polices and contractual obligations with the following policies:

1. Ensure that information is accessible only to those authorized, and required in the course of their duties, to have access (Access Control)
2. Ensure customer data privacy and continued compliance with federal and regional privacy regulations (e.g., FERPA, COPPA, CCPA, NY Ed Law 2D) (Data Privacy Notice, Data Privacy Policy)
3. Define an information classification scheme describing classes and how information of a class should be managed (Information Classification, Acceptable Use)
4. Address the security of all our services and processes to ensure that risks are identified, and appropriate controls are implemented and documented (Access Control, Risk Management)
5. Ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of the information (Data Privacy, Risk Management, Incident Management, Backup Management)
6. Produce business continuity and incident response plans for strategic services, which will be maintained and tested on a regular basis (Incident Management)
7. Promote this policy and raise awareness of information security for all staff and contractors by requiring regularly scheduled information security training (Security Awareness and Training)

6. Responsibilities

Ultimate responsibility for this policy rests with the CEO of the Company. The Information Systems and Security Administrator is responsible for the production and maintenance of company security policies, the controls to enforce the policies and the provision of advice and guidance on implementation and maintenance.

Directors and managers are responsible for implementing this policy within their area of responsibility, and for ensuring the adherence of their staff to this policy.

It is the responsibility of all staff and contractors to adhere to this policy and all related or supporting internal policies.

It is the responsibility of all staff to promote accuracy of policies and procedures, and to participate in the continual improvement of the Information Security Management System.

All breaches of information security will be reported to the Information Systems and Security Administrator and investigated by the appropriate teams.

The Company reserves the right to inspect any data stored on Company computers or telecommunications systems, or transmitted or received via the Company's networks, while investigating security incidents, or safeguarding against security threats.

Responsibility	**Owner**
Execution, sponsorship and quality assurance of this policy	CEO
Production, maintenance, controls and guidance of this policy	Information Systems and Security Administrator
Ensuring staff have awareness of and adhere to this policy	Department managers
Adherence to policy	All Staff, contractors, and partners.
Accuracy of policies and procedures. Continual improvement of the Information Security Management System	All Staff

7. Document management, continual Improvement

This Information Security Policy will be reviewed annually or sooner if necessary by the Information Systems and Security Administrator to ensure it remains current in consideration of relevant legislation, organizational procedures or contractual obligations. Changes will be agreed upon and approved by the CEO as needed.

8. Change History

Date	**Version**	**Created by**	**Description of change**
			Formatting changes added references to continual improvement. Added prefix 2 to version
			Formatting changes add numbers to statements

		David Miller	
11/14/2024	6	Ben Norman	Updating to current format
3/25/25	7	Ben Norman, Josh Britton	Updating to current standard