Mill Creek Agency Cybersecurity Program

Bryce Thuilot, Chief Information Security Office

03/12/2021

Introduction

This document is written in compliance with *New York State Department Of Financial Services 23 NYCRR 500.* The Mill Creek Agency qualifies for exemptions 500.19 a, 500.19 b, and 500.19 c thus outlined in this document are 500.02- Cybersecurity Program, 500.03- Cybersecurity Policy, 500.07- Access Privileges, 500.09- Risk Assessment, 500.11- Third Party Service Provider Security Policy, 500.13- Limitations on Data Retention, 500.17- Notices to Superintendent, 500.18- Confidentiality, 500.19- Exemptions, 500.20- Enforcement, 500.21- Effective Date, 500.22- Transitional Periods, 500.23- Severability.

This document is to be updated every 6 months by the Chief Information Security Officer, or employee with knowledge of 23 NYCCR 500, and approved by the president.

Definitions

- **QQ Catalyst** - Third party policy/data management system.
- **CISO** - Chief Information Security Officer, as of writing this document the current CISO is Bryce Thuilot.
- **Sensitive information/documents** - Any document/financial record that contains non public information.

Section 1 - Cybersecurity Program

Mill Creek's cybersecurity program is laid out in the following sections, broken down by the requirements needed to be meet by 23 NYCCR 500. This program is meant to be followed by all Mill Creek Agency employees. The policy may only be updated by the CISO and must be approved by the president before implemented.

Section 2 - Cybersecurity Policy

The Cybersecurity policy is based on the Risk Assessment performed in *Section 4*, it is broken down by the sections provided by the DFS 23 NYCRR 500

a. *Information Security & Data-Governance* - All sensitive and non public info must be kept on QQ Catalyst, or in Microsoft Office. No sensitive client data or internal data is to be kept on any computer. Data stored on any Mill Creek Agency device will be policy's of clients and any financial or personal information needed to write a policy. Any personal or financial information of a client, or any Non-Public information will need to be immediately uploaded to QQ Catalyst and deleted securely (moved to 'Trash Can' or 'Recycling Bin' and emptied) once uploaded.

b. *Asset Inventory and Device Management* - All devices that contain Non-Public or client information and/or are used to operate must be approved the CISO. No mobile devices are to be used to store/download any non public information. All devices must be using disk encryption not able to be reset using iCloud or any cloud based service. Passwords for disk encryption will be chosen at random by the CISO and not used for anything else. For all user accounts, passwords bust be changed every **3 months and cannot be the same as the any of the previous 5 passwords**. In addition, all company computers must be running an anti virus (ClamAV) with a scan being required at the first and third Friday of each month. All computer must be checked and updated to latest version of all software used on the first day of each month.

c. *Access controls and identity management* - All Access Control and Identity Management will be handled by our third party software, Microsoft Office and QQ Catalyst. Access to non public information will be given on a need to know basis, given to insurance brokers when needed to write policies and the executive staff.

d. *Business continuity and disaster recovery planning and resources and systems operations and availability concerns* - All sensitive information stored by mill creek must be uploaded to QQ catalyst or Microsoft office in case of a

e.

f. *Systems and application development and quality assurance* - No software developed by Mill Creek is to be used in a production environment or to have any internet facing capabilities. Any software developed by any Mill Creek employee is to be used solely to automate process in the business