Mill Creek Agency Cybersecurity Program

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 Security Officer, or employee with knowledge of 23 NYCCR 500, and approved by the president.

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 CSO 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 - All senestive and non public info must be kept on the company computers, which 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 CSO 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 can being required at the first and third Friday of each month.

b. Data-Governance - Data stored by Mill Creek Agency 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 will need to be deleted securely (moved to 'Trash Can' or 'Recycling Bin' and emptied) 2 months for the date obtained. All Data must be stored on company computers or uploaded to QQ Catalyst (Third party policy/data management system).

c. Asset Inventory and Device Management -