Mill Creek Insurance Agency Cyber Policy

Compliant with 23 NYCRR 500.19

Bryce Thuilot cyber@millcreekagency.com

Last Updated January 7, 2022

Purpose

Securing and protecting the confidentiality, integrity, and availability of information assets is in the public's best interest to ensure the safety and security of critical infrastructure, financial and business transactions, and Nonpublic Information (NPI). Failure to address the risks associated with cybersecurity could result in significant costs to Mill Creek Agency as a result of lost, compromised, or unauthorized use of NPI, legal and regulatory actions, and reputational damage and loss of customers, among other things. Cybersecurity Programs are critical to proactively protecting data, mitigating potential risks, and responding quickly and efficiently to cyber incidents, while maintaining compliance with best practice and regulatory requirements.

The purpose of this Policy is to provide a framework for Mill Creek's Cybersecurity Program, which is a documented set of information security policies, procedures, standards and guidelines. (DFS's Cybersecurity Regulation requires both a Cybersecurity Program (23 NYCRR 500.02) and a Cybersecurity Policy (23 NYCRR 500.03)). Mill Creek's Cybersecurity Program shall provide a roadmap for effective security management practices and controls that protect and maintain the confidentiality, integrity, and availability of Mill Creek's Information Systems and information assets, including Nonpublic Information (NPI).

This Policy will be based upon the findings of Mill Creek's Risk Assessment and will address the following core cybersecurity functions:

- To protect and maintain the confidentiality, integrity, and availability of digital information and related infrastructure assets.
- To manage the risk to Mill Creek of cybersecurity exposure and compromise.
- To assure a secure and stable information technology (IT) environment at Mill Creek.
  - identify, respond to, and recover from events involving the misuse, loss, and/or unauthorized disclosure of Mill Creek's information assets.

- monitor Mill Creek's information systems for anomalies that might indicate a compromise.
- promote and increase awareness of information security at Mill Creek and to decrease the risk of cybersecurity exposure and compromise.

Policy Scope

This Policy covers all of Mill Creek's cybersecurity practices across all areas of its business. All Mill Creek employees, including contractors, third parties, and anyone else with access to Mill Creek's systems and data, are required to comply with this Policy.

Policy Statement

Roles and Responsibilities Mill Creek will designate an individual in a senior leadership position who is responsible for Mill Creek's cybersecurity (Senior Officer). The Senior Officer will: - Implement and maintain a written policy or written policies, approved by a Mill Creek's Senior Management, setting forth the expectations and goals for the protection of Mill Creek's Information Systems and Nonpublic Information (NPI) stored on those systems. - Ultimately be responsible and accountable for Mill Creek's cyber compliance, risk, and resilience. - Oversee and implement Mill Creek's Cybersecurity Program and report to management on Mill Creek's cybersecurity generally. - Conduct a formal, independent review of Mill Creek's Cybersecurity Program and controls at least annually. - Prepare and submit the annual Certification of Compliance required by DFS's Cybersecurity Regulation. - Conduct a cybersecurity Risk Assessment at least annually to inform the design of policy and overall cybersecurity program. - Review cybersecurity policies, standards, guidelines, and procedures annually to ensure Mill Creek's compliance with applicable laws, regulations, and industry best practices.

Mill Creek's employees, contractors, consultants and temporary and part-time workers will: - Ensure Mill Creek's information assets are used solely for the purpose of pursuing Mill Creek's business goals and objectives. - Take reasonable steps to ensure electronic information and assets are not improperly disclosed, modified, or destroyed. - Not deliberately circumvent information security controls and not make Mill Creek resources available to any unauthorized persons. - Report suspicious activity and/or unauthorized access to Mill Creek's Information Systems and/or information immediately to their manager or the Senior Officer.

The Senior Office is Bryce Thuilot cyber@millcreekagency.com as of January 7, 2022.

Cybersecurity Policies to Support the Cybersecurity Program Mill Creek will implement and maintain written policies in support of Mill Creek's Cybersecurity Program. Such policies may include, but are not limited to:

- Access Control
- Asset Device Management
- Data Classification
- Systems & Network Security
- Physical security & Enviornmental Control
- Risk Assessment
- Third Party Service Provider

These policies are all defined later in this document

Training and Awareness

- Mill Creek will ensure all users of Mill Creek's Information Systems and anyone with access to Mill Creek's data understand their roles and responsibilities in safeguarding NPI and other sensitive data and protecting company resources from unauthorized access.
- Mill Creek will provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified in the Risk Assessment as well as risks identified in the media and public sphere.
- Mill Creek's Senior Officer will receive cybersecurity training sufficient to address relevant cybersecurity risks.
- Mill Creek will track and record attendance at training activities and shall retain records of attendance for all members of Mill Creek for audit purposes.

Cybersecurity Governance and Reporting This Cybersecurity Policy leverages roles and responsibilities to support Mill Creek's Cybersecurity Program objectives and strategies, and visibly promotes and provides support for cybersecurity initiatives throughout Mill Creek. Mill Creek's Senior Officer shall report in writing on Mill Creek's Cybersecurity Program and material cybersecurity risks at least annually.

Policy Approval Mill Creek will review this Policy periodically for accuracy, completeness, and applicability, and will revise and approve it annually.

Access Control

Purpose of Policy

The purpose of this Policy is to protect, and reduce risk to, business operations by establishing requirements for creating, maintaining, and controlling access to information assets. This Policy ensures that both the information assets and the information in those assets are adequately protected against unauthorized access.

Policy Scope

This Policy applies to all of Mill Creek's data regardless of whether that data is stored by Mill Creek on-site or by a Third Party Service Provider in a hosted or cloud environment and to all Mill Creek employees, including third parties, contractors, Third Party Service Providers, and anyone else who has, or may have, access to Mill Creek's data and Information Systems.

Access Control

- Access to Mill Creek's Information Systems will be limited solely to users whose business needs, job functions, and responsibilities require such access, or to users on a need-to-know basis.
- The ability to approve additions, changes, and deletions to a user's system access will be limited to specific personnel authorized by Mill Creek and that personnel shall grant such approvals only when necessary for valid business reasons.
- The ability to create, delete, and modify user accounts, as well as to grant access to Mill Creek's protected data and resources will be limited to specific personnel authorized by Mill Creek.
- Access reviews for all users and administrative access to Mill Creek's systems will be conducted periodically and, at a minimum, annually.
- Reported discrepancies in permitted access will be remediated immediately.

Granting & Removing User Access

- A process for establishing, activating, modifying, reviewing, disabling, and removing accounts will be formally documented, implemented, and maintained.
- Whenever there is a change in a user's employment status, that user's access will be reviewed and removed or revised to ensure access is limited to only that needed for legitimate business purposes.
- User access granted to third parties, including access granted to Third Party Service Providers and maintenance accounts, will be reviewed regularly and removed or revised to ensure access is limited only to those third party accounts with legitimate business purposes.

- Guest/anonymous, shared/group, emergency, and temporary accounts will be specifically authorized and monitored.
- Unnecessary accounts will be promptly be removed, disabled, or otherwise secured.
- As a best practice, Mill Creek will require strong passwords for all user accounts.
- Inactive accounts will be disabled after 90 days of inactivity.
- User access will be enabled only during the time period needed and disabled when an account is not in use.
- When an account is in use, access will be monitored.
- Users will be locked out after no more than 10 repeated access attempts.
- Lockout duration will be for a minimum of 10 minutes or until such personnel as authorized by Mill Creek re-enables the user ID.
- A user will be required to re-authenticate and to re-activate the terminal or session if the session has been idle for 60 minutes.
- Users will not be permitted to use generic, shared, or service accounts to login.

Privileged Account Management (Administrative Access)

- The allocation and use of Privileged Access to Mill Creek's Information Systems and services will be restricted and controlled. Special attention shall be given to the allocation of Privileged Access rights, which allow users to override system controls.
- Privileged user accounts will be separate from non-privileged user accounts and privileged user accounts will be used only when Privileged Access is required to complete a specific task or function.
- All of a user's Privileged Access to Mill Creek's Information Systems will be immediately revoked or revised as soon as that user's change in employment status, job function, or responsibilities dictate that the user no longer requires such access.
- No service account will be used by more than one service, application, or system.
- Users with Privileged Access will not extend a user group's permissions if such permissions would provide inappropriate access to any user in that group.
- When technically feasible, all servers, applications, and network devices will contain a login banner that coveys the following:
- This computer and network are provided for use by authorized members of Mill Creek.
- The use of this computer and network are subject to all applicable policies of Mill Creek and any applicable laws and regulations.
- The use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies of Mill Creek, laws, and regulations.
- Any other use is prohibited.

Remote Access

Mill Creek does not currently have remote access capabilities

Asset Device Management

Purpose of Policy

The purpose of this Policy is to protect and preserve Mill Creeks' technology assets, and to ensure the confidentiality, integrity, and availability of Mill Creek's Information Systems, technological resources, and data.

It is critically important for Mill Creek to know the location and status of all of its computers, devices, and other equipment that can be used to access Mill Creek's technology assets, Information Systems, and related resources. In order to do so, Mill Creek will maintain up-to-date inventory lists and asset controls. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols include documenting and supporting recovery and replacement of missing equipment and assets, including documenting and supporting insurance activities related to such equipment and assets. This Policy defines the responsibility of everyone within Mill Creek to ensure asset inventories are current and effective controls are in place to identify, track, manage, and dispose of assets properly.

Policy Scope

This Policy covers all of Mill Creek's cybersecurity practices across all areas of its business. All Mill Creek employees, including contractors, third parties, Third Party Service Providers, and anyone else who is in possession of Mill Creek's equipment and/or assets, are required to comply with this Policy.

Asset Types

Mill Creek will track all of its technology assets, including but not limited to:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Software
- Printers, copiers, fax machines, and multi-function print devices
- Mobile handheld devices such as phones
- Scanners
- Network devices (e.g., firewalls, routers, switches, uninterruptable power supplies, endpoint network hardware, and storage)
- External storage devices (including USB thumb drives)

Asset Tracking Requirements

- Mill Creek will create an asset tracking database to track all of Mill Creek's assets, which will include categories such as:
- Type of asset (hardware such as computer, phone, tablet, and software)
- Make, model, serial number, and descriptor of asset

- Owner of asset
- Location of asset
- In active service or offline and stored
- All information on an asset will be entered and maintained in the Mill Creek's asset tracking database before redeploying an asset.
- Mill Creek will own, be fully licensed, and be in full compliance with licensing entitlements of its software to minimize the risk of legal and regulatory problems.
- A process to identify unauthorized hardware and/or software will be undertaken periodically and, if any unauthorized hardware or software is discovered, immediate action will be taken to remedy the situation.
- Mill Creek's asset tracking database will be reviewed periodically for accuracy and completeness.

Asset Disposal and Repurposing

- Procedures for secure disposal or repurposing of equipment and resources will be established and implemented prior to reassignment, transfer, transport, or surplus.
- Sensitive data will be removed prior to disposal of any asset.
- A data destruction protocol will be established and implemented for data destruction.
- Physical media that is storing confidential, sensitive, Nonpublic Information or Personally Identifiable Information will be destroyed if it is not being reused.

Data Classification

Purpose of Policy

This Policy establishes a framework for identifying, classifying, and securing confidential and sensitive corporate and consumer data such as Personally Identifiable Information (PII), Nonpublic Information (NPI), and Electronic Health Information (ePHI). Mill Creek will classify its data based on its sensitivity, value, and criticality and secure such data appropriately based on its classification.

Policy Scope

This Policy applies to any form of digital data stored on any media used by Mill Creek employees, as well as contractors, consultants, third parties, Third Party Service Providers, and anyone else authorized to access Mill Creek's data.

Roles and Responsibilities

The Senior Officer responsible for Mill Creek's cybersecurity:

- Will work with key stakeholders to ensure Mill Creek's data is reviewed and categorized.
- Will ensure data classification labels are assigned based on data sensitivity and criticality (see data classification table). Mill Creek's data classifications are:
  - High – Restricted
  - Medium – Confidential
  - Low – Public
- Will ensure that data merged or compiled from multiple classification sources is classified at the most secure classification level.
- Will ensure that data containing information with High and Medium classifications is secured pursuant to federal and/or state regulations and guidelines that pertain to Mill Creek.
- Will ensure a set of proper access controls designed to protect each data classification label is implemented and, if feasible, monitored and audited.
- Will ensure regular backups are performed and backups sets are protected.
- Will ensure data classified at Medium or High is encrypted while such data is at rest, in storage, or in-transit, and access logs regarding such information are monitored and reviewed periodically.
- Will ensure the appropriate disposal of data when information is no longer needed or in use.

Data Users

- Will only transfer files between network drives on Mill Creek's internal network. (Mill Creek's email system may not be designed to support the transmission of sensitive data securely.)

- Will secure restricted and confidential data sent or received electronically by not leaving such information in public view and, if possible, by using encryption technology such as a secure web transfer or the Secure File Transfer Protocol.
- Will use data in a manner that is consistent with the purpose intended and comply with all Mill Creek policies applicable to data use.
- Will only share data with those who need to know, and are authorized to use, the information in that data.

With respect to Third Parties:

- Mill Creek will undertake a security review of each Third Party Service Provider (TPSP) that will have access to Mill Creek's data, including an assessment of their security controls, before routinely exchanging data classified as Medium or Low with them.
- Mill Creek will ensure the security of Mill Creek's Information Systems and NPI that are accessible to, or held by, TPSPs.
- Mill Creek will use appropriate measures to ensure that contracts with TPSPs identify which party will be responsible for securing sensitive data in transit, how Mill Creek's data will be secured, and how any specific confidentiality and regulatory obligations will be handled.

Systems & Network Security

Purpose of Policy

The purpose of this Policy is to establish requirements for the protection of Mill Creek's information assets from cybersecurity threats which could compromise Mill Creek's confidential and sensitive data and to ensure secure, reliable network access.

Policy Scope

This Policy covers all Mill Creek cybersecurity practices across all areas of its business. All Mill Creek employees, including contractors, third parties and anyone with access to Mill Creek's data and related assets, are required to comply with this Policy.

Endpoint Protection Policy

- Anti-virus/Anti-malware Protection: Mill Creek will ensure its computing systems implement the following fundamental security controls and practices, including but not limited to:
- Password requirements, including Multi-Factor Authorization (MFA) for remote connections.
- Virus protection.
- Personal firewalls.
- Automatic updates enabled for security updates.
- Protect information assets by taking active measures to detect, prevent, and manage malware and virus intrusions and recover from their effects.
- Anti-virus and anti-spyware will be installed on all of Mill Creek's computing systems.
- A network-based malware detection solution will be used as a compensating control when management recommends not installing anti-virus and anti-malware software on its computing devices.
- Scans of systems to identify and remove unauthorized software will be conducted periodically.
- Anti-malware and anti-spyware will be configured to automatically scan for downloads, email attachments, and browser usage.
- Anti-malware and anti-spyware alerts and logging will be enabled.

Automatic Updates/Patching

- All systems connected to Mill Creek's network will have the latest security patches available from the respective vendors and such security patches will be applied with system security updates set to install automatically.
- If security patches are unable to be installed due to business compatibility issues, Mill Creek will implement mitigating and/or compensating controls, appropriate to address the vulnerability.

Disk Encryption

- Mill Creek's desktops, servers, and mobile devices will employ full disk encryption with an approved software encryption package.

Network Security

Host-based/Personal Firewall

- All Mill Creek computers or computers connected to the Mill Creek network will run a personal firewall with the firewall enabled.

Network-based Firewall/Firewall Router Device

- Mill Creek shall ensure that all external and wireless connections to Mill Creek's networks will pass through a network firewall.
- Mill Creek's firewall rules will restrict inbound and outbound traffic to external or trusted networks.
- Mill Creek shall change all vendor default settings for network-based firewalls (e.g., passwords, wireless encryption keys, Simple Network Management Protocol community strings) will be changed prior to installing equipment in a production environment.
- Mill Creek's firewall rules shall apply a default-deny rule that drops all traffic except traffic that is authorized.
- Mill Creek shall adequately test any change to an external connection to the configuration of the firewall, and personnel authorized by Mill Creek shall document and approve such change.
- Mill Creek shall physically place network-based firewalls within a secure space accessible only to those whose roles and responsibilities permit them to manage the firewall.
- Mill Creek shall ensure network-based firewalls will be configured by a secure, encrypted connection with access restricted only to those whose roles and responsibilities permit them to manage the firewall.
- Mill Creek shall periodically back up network-based firewall configurations and store backups securely and accessible to only authorized personnel.

Wireless Networking

- Wireless networks will be segmented between external guests and internal networks.
- Non-Mill Creek devices are prohibited from connecting to Mill Creek's internal network.
- Users inside the Mill Creek firewall will not connect to the internal network if they are using a bridged wireless connection to connect to an external network.
- Wireless access points or routing devices with wireless capability are not allowed unless approved by the Senior Officer.

- Logical and physical user access to wireless network devices will be restricted to authorized personnel.
- Perimeter firewalls will be implemented and configured to restrict unauthorized access.
- All vendor default settings for wireless devices (e.g., passwords, wireless encryption keys, Simple Network Management Protocol community strings) will be changed prior to installing wireless equipment in a production environment.
- Mill Creek will use wireless security protocols that are of the highest encryption possible.
- Mill Creek will require the use of strong passwords for setting encryption for all wireless SSID and will require passwords to be changed periodically (e.g., every 3 months).
- Wireless device audits will be conducted periodically to determine if any rogue devices exist on the Mill Creek network.
- Findings from wireless device audits will be presented as soon as possible to the Senior Officer and all rogue devices will be documented and removed from the network.
- Wireless routers and access points configurations will be backed up periodically and stored securely with access to the configurations restricted to authorized personnel.

Email Security

- Anti-Spam and anti-phishing software will be installed and implemented at entry/exit points of the network and on computing devices connected to the Mill Creek network.
- Anti-Spam and anti-phishing software will be updated to new releases to ensure Mill Creek is protected from the latest email threats.
- All Mill Creek employees and contractors will attend a phishing awareness and training program at least twice a year.
- Mill Creek will require strong authentication measures, including MFA, for access to cloud email such as Office 365 or Gmail in order to reduce account takeover risk.

Monitoring and Auditing

- Mill Creek will maintain and monitor system and network traffic logs for all network devices and systems for security auditing purposes and legal and regulatory requirements.
- Access to log management systems will be recorded and limited to authorized individuals with a specific need for such access.
- For a period of no fewer than 3 years, Mill Creek will securely maintain systems audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal business operations.

- Mill Creek will reserve the right to monitor, access, retrieve, read, and/or disclose data communications when there is reasonable cause to suspect a policy violation, potential criminal activity, monitoring required by law enforcement, or an appropriate management request.

Physical security & Environmental Controls

Purpose of Policy

The purpose of this Policy is to ensure that Mill Creek provides adequate physical and environmental safeguards to prevent damage and unauthorized access to Mill Creek's Information Systems, information assets, and Nonpublic Information (NPI) as well as other confidential and sensitive data.

Policy Scope

This Policy covers all Mill Creek facilities and all Mill Creek information assets at all of Mill Creek's physical locations.

Physical and Environmental Security Policy

- Mill Creek will prevent unauthorized physical access to, damage to, and interference with Mill Creek's premises and information assets.
- Mill Creek will develop and implement processes, procedures, and guidelines for implementing physical and environmental protections.

Physical Security Perimeter

- Mill Creek will design and implement physical security perimeters to protect areas that contain its Information Systems and confidential and sensitive data.
- Mill Creek's walls shall be physically sound and of stable construct.
- Entry to Mill Creek's premises will be limited to authorized personnel by placing control mechanisms on external doors.
- Doors to Mill Creek's internal areas that contain its Information Systems and confidential and sensitive information (e.g., data center, communication closet, etc.) will be adequately secured.
- Mill Creek will establish, maintain, and review visitor logs periodically, and no less frequently than necessary to ensure effectiveness.
- Visitor access to limited areas will be restricted. Visitors will be escorted, supervised and monitored to ensure they do not access restricted areas or take away any of Mill Creek's technology or information assets.

Protection from Environmental Threats

- Mill Creek will design and implement physical protection against damage from fire, water, flood, earthquake, explosion, civil unrest, and other forms of natural or human-made disasters.
- Emergency procedures will be documented and communicated clearly, and personnel will be trained on what to do in emergencies.
- Fire detection systems will be installed in accordance with requisite laws and regulations and HVAC systems will be configured to shut down upon

fire detection automatically. Mill Creek will use its best efforts to identify and remediate any security threats presented by neighboring premises.

Equipment Protection

- Information Systems will be located away from hazardous processes or materials.
- Mill Creek will provide adequate power supplies and auxiliary power supplies to its Information Systems.
- Mill Creek will adequately protect its Information Systems and any devices with Mill Creek's information assets against damage from exposure to water, smoke, dust, chemicals, electrical supply interference, etc.
- Media containing diagnostic and test programs for malicious code will be checked prior to use and on a regular basis.
- Mill Creek will implement adequate controls to prevent the unauthorized removal of equipment.
- Mill Creek will establish guidelines for eating, drinking, and smoking in the proximity of Information Systems and devices with Mill Creek's information assets.
- Physical access to wireless access points, networking and communication hardware, and telecommunication lines will be restricted.

Clear Desk Policy

- A clear desk policy requiring sensitive information, documents, and media to be stored securely in cabinets or away from public view when not in use will be implemented.
- Sensitive or critical business information will be locked away (ideally in a fire-resistant cabinet) when not in use and when the office is vacated.
- Key locks, encryption, passwords, and other controls will be used to prevent unauthorized access to Mill Creek's data on workstation computers, computer terminals, and other devices used for access to Mill Creek's network .
- The use of photographic, video, audio, or other recording equipment such as cameras in mobile devices that could be used to record confidential and sensitive data will be prohibited unless specifically authorized by the Senior Officer.

Off-Premises Security

- The use of any information asset outside of Mill Creek premises, including assets used for remote workers, is prohibited unless specifically authorized by the Senior Officer.
- Information assets and media taken off the premises will not be left unattended and will be secured at all times.
- Portable computing devices will be carried on person when traveling.

Risk Assessment

Purpose of Policy

The purpose of this Policy is to provide a framework for identifying cybersecurity risks and vulnerabilities so that Mill Creek can implement comprehensive solutions to address those risks and vulnerabilities. A Risk Assessment will ensure Mill Creek is aware of, and can adequately protect itself from, new risks and vulnerabilities that constantly arise with respect to cybersecurity, and to ensure Mill Creek's data and other related assets are protected to the greatest extent possible.

To that end, Mill Creek will conduct a Risk Assessment of its Information Systems which will inform the design of its Cybersecurity Program. Mill Creek will conduct Risk Assessments periodically and update its Risk Assessment as necessary to address changes to Mill Creek's Information Systems, Non-Public Information (NPI), or business operations. Mill Creek's Risk Assessment will be conducted in accordance with this Policy.

Policy Scope

This Policy covers all Mill Creek activities across all areas of its business. It applies to all employees, including contractors, service providers and anyone with access to Mill Creek's data and related assets.

Roles and Responsibilities

Mill Creek leadership will establish criteria for: - Evaluating and categorizing cyber risks and threats facing Mill Creek. - Assessing the confidentiality, integrity, and availability of Mill Creek Information Systems and its technology assets, including all data and NPI. - Mitigating or accepting risk identified by the Risk Assessment. - Evaluating the adequacy of existing controls in the context of identified risks. - Updating the Risk Assessment at least annually to address new risks resulting from changes to Information Systems, business operations, or new products and services.

Risk Assessment

The Risk Assessment will assist Mill Creek in understanding, managing, controlling, and mitigating cyber risk by establishing a formal set of guidelines to: 1. Identify and Prioritize Assets. 2. Identify Threats 3. Identify Vulnerability 4. Determine Likelihood and Impact 5. Determine Inherent Risks 6. Analyze Controls 7. Determine Control Effectiveness 8. Analyze Residual Risks 9. Document Results

Identifying and Prioritizing Assets

The process of discovering, recognizing, and documenting assets is the first step in risk identification. Risk identification is essential because the risk that is identified can be assessed and subjected to appropriate mitigation. When assets are not identified, management cannot adequately evaluate, prevent, or minimize cyber risk that can damage both Mill Creek and Mill Creek's customers whose private information may be revealed and/or stolen for illicit purposes.

Mill Creek will create a list of all information assets. Information assets may include tangible items such as servers and workstations and non-tangible digital assets such as sensitive data, NPI and Personally Identifiable Information (PII). For each asset, Mill Creek will compile the following information, as applicable:

- Hardware (such as servers, workstations, firewalls, wireless routers, mobile phones, printers, copiers, uninterruptible power supply (UPS), power generators)
- Software (such as operating systems, firmware, Outlook, Adobe Acrobat)
- Applications (such as Exchange)
- Cloud providers (such as Office 365)

Mill Creek will define a standard for determining the importance of each asset. An overall asset's monetary value may take into account replacement costs, profitability, and legal or regulatory importance. Once Mill Creek has defined a standard, it will be formally incorporated into the Risk Assessment process.

Identify Threats

Threats are anything that could cause harm to an organization. Every Risk Assessment should uncover some basic threats. Additional threats found will depend on the size, type of business, and systems used by an organization. Common threat types include:

- Unauthorized access (malicious or accidental): This could be from a hacking attack/compromise, malware infection, or insider threat.
- Misuse of information (or privilege) by an authorized user: This could result from unapproved use of data or changes to data made without approval.
- Data leakage or unintentional exposure of information: This could result from permitting the use of unencrypted portable storage devices without restriction, inadequate retention and destruction practices, transmitting NPI unsecured, or accidentally sending sensitive information to the wrong recipient.
- Loss of data: This can happen when an organization does not have adequate backup and recovery processes.
- Disruption of service or productivity: This includes the inability to access resources due to natural disasters such as floods, hurricanes, and pandemics or due to human-made disasters such as hardware failure from outdated hardware or the physical theft of a computer or server, etc.

Mill Creek will identify all possible threats to the security of its information assets and address those threats that have a reasonable likelihood of adversely impacting its business.

Identify Vulnerability

A vulnerability is a weakness that can enable a threat to harm an organization. Vulnerabilities can be identified through analysis, audit reports, vulnerability assessments, and tabletop exercises. Examples of threats and corresponding vulnerabilities are:

Threat	Vulnerability
Data leakage or unintentional exposure of information	Unencrypted portable storage with sensitive information was stolen
Loss of data	Backups tapes from last week did not complete
Disruption of service or productivity	Pandemic prevents access to office

Mill Creek will identify all vulnerabilities and address those vulnerabilities that have a reasonable likelihood of adversely impacting its business.

Likelihood and Impact

Mill Creek will determine the likelihood and impact of all vulnerabilities by assessing the probability that a vulnerability might actually be exploited and the impact that such an exploitation would have on Mill Creek if the asset is compromised, lost or damaged. Mill Creek will use the categories High (highly probable, with significant economic and reputational damage,), Medium (probable, with moderate impact), and Low (highly unlikely, with minimal impact) to determine the likelihood of an attack or other adverse event. Inherent Risk

To have a complete view of risk, Mill Creek will review and consider how to respond in worst-case scenarios should any controls fail. Inherent risk is the initial risk that exists when an organization has not implemented controls to reduce the likelihood of a threat exploiting a vulnerability, or to mitigate a risk event's severity. Factoring inherent risk determines how an organization prioritizes risk response efforts by addressing those risks that significantly impact the organization. Mill Creek will use the categories High, Medium, and Low to determine inherent risk. Analyze Controls

Cybersecurity controls are the countermeasures that Mill Creek will implement to detect, prevent, reduce, or counteract security risks. They are the measures that a business deploys to manage threats targeting computer systems and networks. Mill Creek will analyze cybersecurity controls to minimize or eliminate

the probability that a threat will exploit a vulnerability. Controls can either be technical or non-technical. Non-technical controls are management and operational controls, such as administrative policies, procedures, and standards. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware. Encryption, Multi-Factor Authentication (MFA), and firewalls are common technical controls. Mill Creek shall identify controls that will prevent, mitigate, detect, or compensate for addressing an identified vulnerability.

Determine Control Effectiveness/Residual Risk

Once Mill Creek has identified controls that will prevent, mitigate, detect, or compensate for addressing an identified vulnerability, Mill Creek will assess the control's effectiveness to determine residual risk. Mill Creek will categorize a control's effectiveness as Satisfactory, Satisfactory with Recommendations, Needs Improvement, or Inadequate. A certain amount of Residual Risk will remain in place even after Mill Creek implements security measures and controls. Mill Creek will use the categories High, Medium, and Low to assess the remaining risk once controls have been applied.

Document Risk Assessment Results

The final step in the Risk Assessment process is to record results in order to make appropriate decisions with respect to strategic planning, budget, policies, procedures, and other matters. Mill Creek's recorded results will identify assets and describe the corresponding threats and vulnerabilities to derive risk value representing Mill Creek's inherent risk. Mill Creek's recorded findings also will identify and assess the effectiveness of the set of controls or control recommendations to determine the residual risk to the organization.

In conclusion, Risk Assessments are a fundamental part of a risk management process because they help an organization arrive at an acceptable level of risk and draw attention to potential or required control measures. The Risk Assessment process is iterative and must be conducted and reviewed regularly to ensure the Cybersecurity Program's relevancy.

Example Risk Assessment

Assest	Threat	Vulnerability	Impact	Likelyhood	Control Mechanism
iMac	Malware	Phising Email	High	Low	Anti-virus

Third Party Service Providers

Purpose of Policy

This Policy shall establish requirements by which Mill Creek will manage security risks associated with Third Party Service Providers (TPSPs) and all other contracted provider arrangements. The intent is to ensure that the security of Mill Creek information and information assets are not reduced when exchanging information with third parties or by the introduction of third party products or services into the Mill Creek environment.

Policy Scope

This Policy covers all Mill Creek TPSPs and all other contracted provider arrangements. All Mill Creek employees, including third parties and contractors, are required to comply with this Policy.

Risk Management

Mill Creek shall manage and address the security risk of TPSPs that may have access to Mill Creek's data or provide products or services to Mill Creek.

Objectives

- Mill Creek will establish a Risk Assessment process to identify, measure, mitigate, and monitor risks to Mill Creek's data, information systems, and Nonpublic Information (NPI) accessible to, or held by, third parties.
- Mill Creek will establish a due diligence process for prospective TPSPs, which addresses, at a minimum, a TPSP's:
- financial condition,
- reputation,
- cybersecurity practices,
- insurance coverage,
- critical third parties, and
- strategic partners.
- Mill Creek will perform a periodic review of adherence to Service Level Agreements (SLAs), cybersecurity measures, and contractual and regulatory requirements.
- Mill Creek will maintain a current and accurate listing of all TPSPs and conduct a Risk Assessment of each one periodically.
- The Senior Officer of Mill Creek responsible for Mill Creek's cybersecurity will inform senior management, and the Board of Directors if one exists, of the risks associated with outsourcing agreements to ensure effective risk management practices.

Third Party Risk Assessment

- Mill Creek will establish a checklist or questionnaire to identify the risks of using a TPSP to determine if such third party's practices could have a negative impact on Mill Creek. Elements of a TPSP questionnaire should include the TPSP's:
- Need to access NPI, Personally Identifiable Information (PII), or Electronic Health Information (ePHI)
- Need to access financial or confidential data
- Need to access Mill Creek's internal network
- Audit program or SSAE18 report
- Cybersecurity Program
- Vulnerability and penetration testing program
- Cybersecurity insurance or other related insurance
- Involvement in any recent cyberattack or data breach
- Compliance with federal and state laws and regulations
- Mill Creek will review the checklist or questionnaire to evaluate and mitigate risks if possible and to decide whether to pursue the relationship with the third party.
- Mill Creek will conduct further due diligence to analyze whether the TPSP meets Mill Creek's needs and regulatory requirements.

Third Party Review

- Mill Creek will have a review program to ensure TPSPs are delivering the quantity and quality of services expected and/or agreed upon.
- Mill Creek will monitor the key aspects of its relationships with third parties, including the security controls and financial strength of each third party, and the impact of any external events on its relationships with third parties. Third Party Tracking
- To increase monitoring effectiveness, Mill Creek periodically will rank TPSP relationships according to risk to determine which service providers require closer monitoring.
- Mill Creek will base its rankings on the relationship's residual risk after analyzing the quantity of risk relative to the controls over those risks.
- Relationships with third parties that Mill Creek has determined to be higher risk will receive more frequent and stringent monitoring of their performance (financial and/or operational), and more frequent independent control validation reviews.

Third Party Service Reporting

- Mill Creek will monitor the service, reports, audits, and records provided by a TPSP and review them at intervals that will be based on their risk ranking.
- Mill Creek will conduct independent audits to ensure TPSPs are complying

with their agreements and all requisite laws and regulations.

- Mill Creek will conduct regular meetings as required by SLAs and TPSP agreements to review reports, audit trails, security events, operational issues, failures, and disruptions, and will investigate and resolve identified issues.
- Mill Creek periodically will audit network connections with TPSPs to ensure that the connections are appropriate and meet all agreed upon requirements.

Glossary

Business Continuity Plan A documented set of predetermined processes and procedures that describe how a company critical business processes will be sustained during and after a significant disruption such as a natural or human-induced disaster.

Certificate of Compliance A written statement certifying that an organization is in compliance with the requirements applicable to it as set forth in the Cybersecurity Regulation promulgated by the New York Department of Financial Services (DFS). The Certificate of Compliance must be signed by a senior officer of an organization and submitted to DFS every year by April 15.

Cybersecurity Program A documented set of information security policies, procedures, guidelines, and standards that provides effective management practices and controls to ensure the confidentiality, integrity, and availability of an organization's assets and data.

DFS's Cybersecurity Regulation A set of regulations promulgated and enforced by the New York Department of Financial Services (DFS) regarding cybersecurity. The regulations can be found in Part 500 of Title 23 of New York Codes, Rules and Regulations (NYCRR).

Disaster Recovery Plan A documented set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Incident Management A structured methodology for handling security incidents, breaches, and cyber threats through a well-defined process that effectively identifies and minimizes the damage of a cyber event.

Information Asset Information or data that is of value to the organization, including such information as patient records, nonpublic information, intellectual property, or customer information.

Information Systems A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

Nonpublic Information (NPI) All electronic information that is not publicly available information such as business-related information which unauthorized disclosure, access or use of which would cause a material adverse impact to the operations or security of the business. A combination of any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual. Any health care information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual.

Risk Assessment The combined effort of: identifying and analyzing potential events that may negatively impact an organization's assets, and/or the environment; making judgments based on the likelihood and impact of the negative events; and addressing those events in a systematic way.

Risk Management The identification, evaluation, and prioritization of risks followed by coordinated application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Third Party Service Provider (TPSP) A person or entity that provides services and maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the organization. A third party is not an affiliate of Mill Creek Agency.

Vulnerability Management The systematic practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.