VISCOSITY SYSTEM AND DATA INTEGRITY

Author:	Viscosity North America
Creation Date:	January 2020
Last Updated:	April 2026
Document Ref:	System/Data Integrity
Version:	2026

VISCOSITY
NORTH AMERICA

1 DOCUMENT CONTROL

1.1 Change Record

Date	Author	Version	Change Reference
January 2020	Leisa Pitner	Final 2020	Created, revised and in use
February 2021	Leisa Pitner	Final 2021	Documentation review, no changes created at this time.
December 2022	Leisa Pitner	Final 2022	Documentation review, new corporate address
December 2023	Leisa Pitner	Final 2023	Review, no change
February 2025	Leisa Pitner	Final 2025	Review, no change
April 2026	Leisa Pitner	Final 2026	Review, no change

1.2 Reviewers

Date	Name	Position
January 2020	Charles Kim	CEO
January 2020	Justin Nugent	CSO
January 2020	Leisa Pitner	Director of Management and Coordination and Delivery Assurance
February 2021	Leisa Pitner	Director of Management and Coordination and Delivery Assurance
December 2022	Justin Nugent	CSO
December 2024	Justin Nugent	CSO
February 2025	Justin Nugent	CSO
April 2026	Justin Nugent	CSO

Contents

2 INTRODUCTION

2.1 Purpose

This policy establishes the Enterprise System and Data Integrity Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The system and information integrity policy govern Viscosity North America security best practices for system configuration, security, and error handling.
The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by Viscosity North America. Information not specifically identified as the property of other parties, which is transmitted or stored on Viscosity North America IT resources (including e- mail, messages, and files) is deemed the property of Viscosity North America. All users (Viscosity North America employees, contractors, vendors, or others) of IT resources are responsible for adhering to this policy.

2.2 Policy Statement

Viscosity information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems which process it (computers, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on the need-to-know. Management must devote time and resources to ensure that information is properly protected.

All employees, consultants, and contractors must be provided with supporting reference materials to allow them to properly protect and otherwise manage Viscosity information assets. Materials should communicate that information security is an important part of Viscosity's business and must be viewed like other on-going business functions such as accounting and marketing.

The Managing Partners are responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.
All employees are expected to be aware, familiarized, and in compliance with the boundaries of Viscosity North America System and Data Integrity Policy when updates to the policy have been notified by email, web, or physical postings. Under no circumstance should there be any circumvention of Viscosity's policy without the written approval of Viscosity Managing Partners, who serves as the governance for this policy. Non-compliance with this may result in disciplinary action up to and including termination.

2.2.1 GUIDING PRINCIPLES

- Senior Management are committed to and support the successful establishment and continuance of information security management programs.
- Policy is defined and published regarding information security management within Viscosity North America.
- All employees are made aware and required to adhere to defined security management standards.
- No less than annual audit will ensure compliance with the policy.
- Ensure the continued availability of information systems.
- Ensure the integrity of the information stored on computer systems.
- Preserve the confidentiality of sensitive data.
- Ensure conformity to applicable laws, regulations, and standards.
- Ensure adherence to trust and obligation requirements in relation to any information relating to an identified or identifiable individual in accordance with its privacy policy or applicable privacy laws and regulations.
- Preserve the confidentiality of sensitive data in store and in transit.
- Incident handling and response is documented, managed, and assessed annually to confirm that response is conducted.

2.2.2 GOVERNANCE

- This document is owned and managed by the Chief Security Officer and any changes to this policy require approval of that role holder. The document will be reviewed annually for validity against the current business direction.

3 POLICY PROVISIONS

3.1 Access Management

3.1.1 LOGICAL ACCESS MANAGEMENT

All Viscosity North America Business Systems access is:

- Established, managed, and controlled at logical level.
- Based on least privilege and segregation of duties.
- Consistent with the recipient's authorization to access the data
- Granted to fulfill an operational requirement
- Limited to only necessary data
- Granted only for as long as it is needed
- Compliant with laws, regulations, policies, contracts, and other governing requirements.

3.1.2 PHYSICAL ACCESS MANAGEMENT

All Viscosity North America Sites access must:

- Restrict access limited to only those individuals authorized by management.
- Employee keypad access is required, with unique passcodes assigned to each employee to track arrival and departure.
- Ensure all visitors have an escort for the duration of their visit.

3.2 Vulnerability and Threat Management

3.2.1 MALICIOUS CODE PROTECTION

All Viscosity North America Business Systems must:

- Employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., email, removable media, and malicious websites) on the network to detect and eradicate malicious code.

- Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.
- Configure malicious code protection mechanisms (e.g., real-time scans, periodic scans, malicious code detection) to protect company information systems and assets.
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information asset.

3.2.2 SOFTWARE AND INFORMATION INTEGRITY

All Viscosity North America Business Systems must detect unauthorized changes to software within their information asset.

- All Viscosity North America Business Systems must employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. In addition, Viscosity North America Business Systems must update spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
- All Viscosity North America Business Systems must restrict the capability to input unauthorized information into the information asset to authorized personnel.
- All Viscosity North America Business Systems must check the validity of information inputs for company information assets.

3.2.3 INFORMATION SYSTEM MONITORING

All Viscosity North America Business Systems must:

- Monitor events on the information asset and detect information asset attacks.
- Identify unauthorized use of the information assets.
- Deploy monitoring devices
- strategically within the information asset to collect organization-determined essential information, and
- at ad-hoc locations within the system to track specific types of transactions of interest to the organization. o Heighten the level of information asset monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

3.2.4 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

All Viscosity North America Business Systems must:

- Receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
- Generate internal security alerts, advisories, and directives as deemed necessary.
- Disseminate security alerts, advisories, and directives to key system owners and stakeholders.
- Implement security directives in accordance with established time or notify the issuing organization of the degree of noncompliance.
- Security Functionality Verification: All Viscosity North America Business Systems must verify the correct operation of security functions on an annual basis and notify the system administrator when anomalies are discovered to ensure timely corrective action.

3.2.5 ERROR HANDLING

All Viscosity North America Business Systems must have company information assets that:

- Identify potentially security-relevant error conditions.
- Generate error messages that provide information necessary for corrective actions without revealing company sensitive information in error logs and administrative messages that could be exploited by adversaries.
- Reveal error messages only to authorized personnel.

3.3 Incident Management

Incident management ensures normal service operations are restored as quickly as possible and minimizes the adverse impact on business operations ensuring the best possible levels of service quality and availability are maintained. Viscosity North America Incident Management will:

- Ensure all incidents are detected, recorded and appropriate group(s) alerted.
- Classify all incidents, assigning impact and urgency, thereby defining the priority.
- Retain the collateral for all investigations and diagnosis to assist in improved response times.
- Resolve the incident using the solution/work around or engage necessary resources via defined escalation practices with vendors.
- Provide timely communications for the duration of the incident, insuring critical stakeholders are aware

3.3.1 PROBLEM MANAGEMENT

Problem management minimizes the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure and prevents recurrence of Incidents related to the errors. Viscosity North America Problem Management will:

- Ensure problems are tracked from identification through resolution.
- Identifying trends to proactively prevent recurrence of past problems and prevent new ones.
- Maintain problem logs regarding known issue and if any, known work around solutions to mitigate risk and minimize impact.
- Perform post reviews to constantly improve problem management.

3.3.2 FLAW REMEDIATION

All Viscosity North America Business Systems must:

- Identify, report, and correct information system flaws.
- Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.
- Incorporate flaw remediation into the organizational configuration management process.

3.4 Information Output Handling and Retention

All Viscosity North America Business Systems must handle and retain both information within and output from the information system in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements.

4 CONTACT US

If you believe your Personal Information has been used in a way that is not consistent with this Policy or your specified preferences, or if you have further questions related to this policy, please contact us. Written inquiries may be addressed to:

Chief Security Officer, Viscosity North America
3016 Communications Parkway, Suite 200
Plano, TX. 75093

4.1 Policy Updates

Viscosity reserves the right to amend Viscosity's Management and Coordination Policy at any time as deemed necessary to meet our business direction.

4.2 Exceptions

No exceptions to this policy will be allowed unless specifically granted by the employee's manager, and Viscosity Executive Management.

4.3 Approvers

Charles Kim, Founder and CEO
Jerry Ward, Co-Founder and COO
Justin Nugent, Co-Founder and CPO

4.4 Corporate Headquarters

Viscosity's corporate headquarters are located at:

3016 Communications Parkway, Suite 200
Plano, TX. 75093

Tel: +1.469-444-1380 or online at http://www.viscosityna.com/contact-us/