VISCOSITY AUDIT AND ACCOUNTABILITY POLICY

Author:	Viscosity North America
Creation Date:	January 2020
Last Updated:	April 1, 2026
Document Ref:	AuditPolicy
Version :	2026

1 DOCUMENT CONTROL

1.1 Change Record

Date	Author	Version	Change Reference
January 2020	Leisa Pitner	Final 2020	Document creation, 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	Documentation review, new corporate address
February 2025	Leisa Pitner	Final 2025	Documentation review, new corporate address
April 2026	Leisa Pitner	Final 2026	Documentation review, new corporate address

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	Leisa Pitner	Director of Management and Coordination and Delivery Assurance
December 2025	Justin Nugent	CSO
February 2025	Justin Nugent	CSO
April 2026	Justin Nugent	CSO

Contents

2 INTRODUCTION

2.1 Purpose

This policy document provides Viscosity security policy statements and commitment to develop, implement, and maintain an Information Security Audit and Accountability Policy and procedures to protect information and critical resources from a wide range of threats to ensure business continuity, minimize business risk for information systems and data of which the State is considered the owner.

2.2 Policy Statement

All employees, consultants, and contractors must be provided supporting reference materials to allow them to properly protect and otherwise manage Viscosity policies. 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 Audit and Accountability 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 serve as the governance for this policy. Non-compliance may result in disciplinary action up to and including termination.

2.2.1 GUIDING PRINCIPLES

- Senior Management is committed to and in support of the successful establishment and continuance of an information security management program.
- 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 are 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 AUDIT EVENTS – REVIEW AND UPDATES

Viscosity shall review and update the audited events annually or when a major change to the information system occurs. Over time, the events that agencies believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

3.1.1 CONTENT OF AUDIT RECORDS

Information systems shall be configured to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

At a minimum, the following elements shall be identified within each audit record:

- Date and time when the event occurred
- Software/hardware component of the information system where the event occurred
- Source and destination network addresses
- Source and destination port or protocol identifiers
- Type of event that occurred
- Subject identity (e.g., user, device, process context)
- The outcome (i.e., success or failure) of the event
- Security-relevant actions associated with processing

3.1.2 POLICY

Viscosity has chosen to adopt the Audit and Accountability principles established in NIST SP 800-53 "Audit and Accountability Control Family guidelines," as the official policy for this domain. The following subsections outline the Audit and Accountability standards that constitute Viscosity policy. Each Viscosity Business System is then bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

- **AU-1 Audit and Accountability Procedures**: All Viscosity Business Systems must develop, adopt, or adhere to a formal, documented audit and accountability procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- **AU-2 Auditable Events**: All Viscosity Business Systems must:
  Determine that the information asset must be capable of auditing the following events: **User Access and User Transactions**.
- Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

- Provide a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents. o
  Determine that the following events are to be audited within the information asset.
- **AU-3 Content of Audit Records**: All Viscosity Business Systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
- **AU-4 Audit Storage Capacity**: All Viscosity Business Systems must allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.
- **AU-5 Response to Audit Processing Failures**: All Viscosity Business Systems must alert designated organizational officials in the event of an audit processing failure. In the event of an audit processing failure, Viscosity Business Systems must configure the audit log to (1) stop generating audit records or (2) overwrite the oldest audit records.
- **AU-6 Audit Review, Analysis, and Reporting**: All Viscosity Business Systems must review and analyze information asset records periodically for indications of inappropriate or unusual activity, and report findings to designated organizational officials. In addition, Viscosity Business Systems must adjust the level of audit review, analysis, and reporting within the information asset when there is a change in risk to organizational operations, organizational assets, individuals, other organizations due to credible intelligence.
- **AU-7 Audit Reduction and Report Generation**: All Viscosity Business Systems must provide audit reduction and report generation capability for company information assets.
- **AU-8 Time Stamps**: All Viscosity Business Systems must use internal system clocks to generate time stamps for audit records to facilitate logging and monitoring.
- **AU-9 Protection of Audit Information**: All Viscosity Business Systems must protect audit information and audit tools from unauthorized access, modification, and deletion.
- **AU-10 Non-Repudiation**: All Viscosity Business Systems must protect against an individual falsely denying having performed a particular action on company information assets.
- **AU-11 Audit Record Retention**: All Viscosity Business Systems must retain audit records for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
- **AU-12 Audit Generation**: All Viscosity Business Systems must:
  - Provide audit record generation capability for the list of auditable events defined in AU-2 for information assets.
  - Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.
  - Generate audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

4 CONTACT US

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 CSO

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/