VISCOSITY INCIDENT RESPONSE PLAN

Author:	Viscosity North America
Creation Date:	March 2012
Last Updated:	April 2026
Document Ref:	Incident Plan
Version:	2026

VISCOSITY
NORTH AMERICA

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 incident response plan to develop, implement, and maintain policy and procedures to protect information and critical resources from a wide range of threats in order 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 incident response plan when updates to the policy have been notified by email, web, or physical postings. Under no circumstance should there be any circumvention Viscosity's policy without the written approval of Chief Security Officer, who serves as the governance for this policy. Non-compliance to this may result in disciplinary action up to and including termination.

2.2.1 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 INCIDENT RESPONSE DISCOVERY

The person who discovers the incident will call the duty manager on call. The known sources should be provided with a contact procedure and contact list. The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the incident response form, which covers the following items:

- The name of the caller.
- Time of the call.
- Contact information about the caller.
- The nature of the incident.
- What equipment or persons were involved?
- Location of equipment or persons involved.
- How the incident was detected.

3.1.1 CONTACTED MEMBERS RESPONSE

The response team will meet or discuss the situation over the telephone and determine a response strategy.

- Is the incident real or perceived?
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?
- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care?
- What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

3.1.2 INCIDENT TICKET

An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

- Category one - A threat to public safety or life.
- Category two - A threat to sensitive data
- Category three - A threat to computer systems
- Category four - A disruption of services

3.1.3 REVIEW

Team members will review system logs, look for gaps in logs, review intrusion detection logs, and interview witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

3.1.4 RECOMMENDATIONS

Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

3.1.5 APPROVAL

Upon management approval, the changes will be implemented.

3.1.6 AFFECTED SYSTEMS

Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

- Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct events and to the proper level.

3.1.7 DOCUMENTATION

The following shall be documented:

- How the incident was discovered.
- The category of the incident.
- How the incident occurred, whether through email, firewall, etc.

- Where the attack came from, such as IP addresses and other related information about the attacker.
- What the response plan was.
- What was done in response?
- Whether the response was effective.

3.1.8 EVIDENCE PRESERVATION

Make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

3.1.9 NOTIFY PROPER EXTERNAL AGENCIES

Notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

3.1.10 ASSESS DAMAGE AND COST

Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

3.1.11 REVIEW RESPONSE AND UPDATE POLICIES

Plan and take preventative steps so the intrusion cannot happen again.

- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion and then consider what could be changed to ensure that the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident-response procedures detailed, and did they cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

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/