Table of Contents

Background

Verisk is committed to promoting honesty, integrity, accountability and trust in the work environment. This Policy supports this commitment by providing the necessary vehicles to report concerns that may threaten Verisk's core values, provide a safe and secure method to protect reporters from retaliation, or any backlash or scrutiny and incorporate global laws and regulations that satisfy the requirements of all Verisk's locations.

Purpose

To establish governance and procedures for the receipt and handling of reported concerns, including those submitted by employees, as to matters that may arise or are alleged to arise, that conflict with Verisk's core values, Code of Business Conduct and Ethics Policy, other Verisk Policies, or global and local laws and regulations.

Scope

This Whistleblower Policy applies to all Verisk Analytics corporate subsidiaries and affiliates ("**Member Companies**"), as well as their directors, officers, employees, contractors and subcontractors acting or operating on Verisk's behalf. The Policy provides guidance for interested parties, including employees, to raise concerns regarding fraud, corruption, money laundering or intentional error as it relates to Verisk's accounting, auditing, financial or internal controls, violations of Verisk's Code of Business Conduct and Ethics Policies, matters effecting employee safety and physical security, data privacy and cybersecurity matters and other behavior that conflicts with the values of our Company or any local law or regulation.

Verisk employees should report information or reasonable suspicions concerning any actual or potential unlawful action or inaction in the fields outlined in the Policy, which occurred or may occur, of which they are or have been made aware.

Policy Statement – No Retaliation

Verisk does not tolerate retaliation against anyone who speaks up in good faith to report concerns about behavior that does not follow our Verisk Policy, Code of Business Conduct and Ethics or the law. This includes concerns about any observed, suspected, illegal, unethical behavior, or Code of Business Conduct and Ethics-related violations. Any employee who raises a good faith concern through these methods should do so without fear of dismissal or retaliation of any kind. Employee submissions will be maintained anonymously where allowed by law. Verisk will maintain confidentiality, including the identity of the individual raising the concern, except where required to be disclosed by law or to legal counsel. The Company will not retaliate or discriminate against any individual who raises a concern in good faith.

Requirements

Raising a Concern

Verisk has appointed a third-party independent supplier to receive reports online and by telephone. Concerns related to the matters list above or any matter that may substantially impact Verisk' business, can be submitted using the below channels:

- a web-based report at https://verisk.ethicspoint.com/
- a telephone report, made to one of your country helpline numbers available at https://verisk.ethicspoint.com/

The Whistleblower will be provided with a unique report key enabling access to the system and providing an opportunity to review, check, correct and approve the report.
Concerns raised through these channels should include sufficient information and detail to enable a thorough investigation. Confidentiality will be maintained to the fullest extent possible, consistent with all legal and comprehensive review requirements.

Anonymous Reporting

Employees may choose to report a concern and remain anonymous. This may limit the depth of investigation and follow-up that can be provided for the case. Such reports shall be processed in the same manner as signed reports, except of an acknowledgement and feedback giving steps.

Handling Concerns

- Once the report is submitted:
  - an automated acknowledgement will be sent to the reporter
  - depending on the report category, a notification will be sent to designated member(s) of the Report a Concern Review Committee
- An individual responsible for the case intake will perform the initial review with an oversight by the General Counsel or an appropriate designee in the Legal Department. If the matter requires escalation, the General Counsel may, at any time discuss the concerns raised with the Audit Committee or the Chair of the Audit Committee.
- After initial review, the General Counsel may determine whether the matter warrants an investigation and will oversee any such investigation. If the matter requires escalation, the General Counsel will discuss at any time the concerns raised with the Audit Committee or the Chair of the Audit Committee.
- The investigation will be performed by the individual who received the report, or by the member(s) of respective department(s) assigned to perform the task. Depending on the subject matter, concerns may be handled solely or in collaboration with multiple areas as follows:
  - Accounting, auditing, or internal control matters will be reviewed under the direction and oversight of Internal Audit
  - Data Privacy concerns involving the loss or exposure of PII will be reviewed by the Privacy Department
  - Cybersecurity concerns will be reviewed by Information Security Department
  - Ethical and compliance concerns or violations of Policy will be reviewed by Corporate Compliance Governance
  - Employee relations concerns will be reviewed by Employee Relations (HR)
  - Employee Safety and Physical Security concerns will be reviewed by Global Protection Services
  - Violations of laws and regulations will be reviewed by Legal Department
- The person(s) authorized to conduct the investigation will report to the General Counsel in a timely manner all findings of fact, conclusions, and proposed recommendations for remedial actions, if any
- Prompt and appropriate corrective action will be taken to resolve and proactively prevent further matters, where applicable to the extent warranted in the judgment of the General Counsel and, if required in consultation with the Audit Committee.
- The Corporate Compliance Governance team will log and triage all complaints, tracking their receipt as well as any case investigation, updates and resolution, and shall prepare a quarterly summary report for the Report a Concern Review Committee. Copies of complaints and log or tracking materials will be maintained in accordance with the Company's policy regarding document retention.
- Reporters will be notified of the outcome of the investigation, conclusions and remedial actions applied without undue delay. Where possible, designees should also provide updates during the investigation.
- The Report a Concern Review Committee shall prepare quarterly reporting summaries for the General Counsel to include in reporting to the Risk and Audit Committees of the Board of Directors.

Roles and Responsibilities

Business Unit (BU) Head

- Ensure Business Unit adheres to the Whistleblower Policy and all supporting standards and processes
- Ensures all BU employees complete required training that pertains to reporting concerns, at time of hire, at least annually, and as required

Compliance Monitoring & Oversight ("CM&O")

- Investigate potential violations of the Whistleblower Policy
- Oversee the logging, triage, tracking receipt, investigation, updates and resolution, and preparation of a quarterly summary report for the Report a Concern Review Committee.

Corporate Compliance Governance

- Maintain and annually review the Whistleblower Policy and its supporting standards, authorizations, processes and guidance
- Maintain and provide appropriate communications and training concerning all Whistleblower Program policies, standards and processes to all Verisk personnel.
- Perform initial case review and notify the appropriate investigative area of concern
- Log and triage all complaints, tracking receipt, investigation, updates and resolution, and prepare a quarterly summary report for the Report a Concern Review Committee.
- Maintain copies of complaints and log or tracking materials in accordance with the Company's document retention policy.

Employees

- Report concerns of policy violations and unethical behaviors to any of the Report a Concern Hotline/Whistleblower intake methods.
- Complete required training pertaining to reporting concerns, at time of hire, at least annually, and as otherwise required

General Counsel

- Communication reported case trends to the Senior Operating Committee on a semiannual basis or as otherwise requested.
- After initial review and as appropriate, determine if the matter warrants investigation, oversee any such investigation, escalate as/if necessary

Investigation Areas (including without limitation Corporate Compliance Governance, Internal Audit/Compliance Monitoring & Oversight, Global Protection Services, Human Resources, Privacy and Security):

- Investigate all cases (that fall under each purview) received through the Report a Concern Hotline/Whistleblower intake method and all subsequent methods of reporting concerns of policy violations and unethical behaviors
- Report to the General Counsel in a timely manner all findings of fact, conclusions, and proposed recommendations for remedial actions, if any
- Take prompt and appropriate corrective action to resolve and proactively prevent further matters
- Communicate with case Reporters, where applicable throughout the investigation lifecycle and to final case resolution.
- At the time of the closure of a case investigation, provide close notes summarizing the action necessary to resolve the case, as well as a designation of the case being substantiated or unsubstantiated.

Legal Department (Legal)

- Provide legal guidance concerning any Whistleblower laws, regulations, activities or processes upon request

Report a Concern Committee

- Oversee the Whistleblower Program and all supporting working groups, processes and initiatives
- Ensure alignment of Whistleblower Program activities with organizational strategies and processes, while maintaining compliance with laws and regulations concerning Whistleblower programs and requirements globally.
- Maintain and annually review the Whistleblower Policy and its supporting standards, authorizations, processes and guidance.
- Maintain and provide appropriate communications and training concerning all Whistleblower Program policies, standards and processes to all Verisk personnel.
- Conduct quarterly meetings to examine cases, discuss process or other recommendations and identify trends in reported cases.

RASCI Chart

Task	Business Unit Head	Compliance Monitoring & Oversight	Corporate Compliance Governance	Employees	General Counsel	Investigation Areas	Legal Department	Report a Concern Review Committee
Oversee the Whistleblower Program and all supporting working groups, processes and initiatives.					I	S		R, A
Ensure Business Unit adheres to the Whistleblower Policy and all supporting standards and processes	R							
Ensure all Business Unit employees complete required training related to reporting concerns on an (at least) annual basis and at time of hire	R							
Ensure alignment of Whistleblower Program activities with organizational strategies and processes, while maintaining compliance with laws and regulations concerning Whistleblower programs and requirements globally.					I	S, C		R, A
Maintain and annually review the Whistleblower Policy and its supporting standards, authorizations, processes and guidance			R, S		I			R, A
Maintain and provide appropriate communications and training concerning all Whistleblower Program policies, standards and processes to all Verisk personnel.			R, S		I			R, A
Conduct quarterly Report a Concern Review Committee meetings to examine cases, discuss process or other recommendations and identify trends in reported cases.						S, C		R, A
Complete required training pertaining to reporting concerns, at time of hire, at least annually	A, I			R				
Report concerns of policy violations and unethical behaviors to any of the Report a Concern Hotline/Whistleblower intake methods.				R				
Perform initial case review and notify the appropriate investigative area of concern			R					
Log and triage all complaints, tracking receipt, investigation, updates and resolution, and prepare a quarterly summary report for the Report a Concern Review Committee.			R					
After initial review and as appropriate, determine if the matter warrants investigation, oversee any such investigation, escalate as/if necessary					R, I		C	
Maintain copies of complaints and log or tracking materials in accordance with the Company's document retention policy.			R					
Communicate reported case trends to the Senior Operating Committee on a semiannual basis or as otherwise requested.					R	S		S, A
Oversee the logging, triage, tracking receipt, investigation, updates and resolution, and preparation of a quarterly summary report for the Report a Concern Review Committee		R, A						
Investigate all cases (that fall under each purview) received through the Report a Concern Hotline/Whistleblower intake method and all subsequent methods of reporting concerns of policy violations and unethical behaviors.						R, A		I
Report to the General Counsel in a timely manner all findings of fact, conclusions, and proposed recommendations for remedial actions, if any						R, A		
Prompt and appropriate corrective action will be taken to resolve and proactively prevent further matters of issue					I	R	C	C, A
Communicate with case Reporters, where applicable throughout the investigation lifecycle and to final case resolution. .						R, A		
At the time of the closure of a case investigation, provide close notes summarizing the action necessary to resolve the case, as well as a designation of the case being substantiated or unsubstantiated.						R, A		
Investigate potential violations of the Whistleblower Policy		R, A	C		A, I			
Provide legal guidance concerning any Whistleblower laws, regulations, activities or processes upon request					I		R, A	

Responsible: Who is responsible for doing a task or process.
Accountable: Who approves the work or process.
Supporting: Who provides support for the work, such as materials or documents.
Consulted: Who provides knowledge, information or expertise to help complete the work, but is not directly performing the tasks and is not responsible/accountable.
Informed: Who needs to know the result of the task/process, but is not actively involved in the work or responsible/accountable.

Definitions

The following defined terms apply to this Whistleblower Policy and its supporting program, standards and processes.

Accounting: The system of recording and summarizing business and financial transactions and analyzing, verifying, and reporting the results; including but not limited to the principles and procedures relating to these activities.

Auditing: The verification of the Company's financial position as disclosed by its financial statements; an examination of accounts to ascertain whether the financial statements give a true and fair-view financial position and profit or loss of the business.

Case(s): A concern that is received through any of Verisk's Whistleblower intake methods.

Compliance: Adherence to law, Verisk's Code of Conduct, culture and values.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes.

Data Privacy: The principle of protecting personal data and sensitive business data, including data that customers and/or third-party contributors license to Verisk and allow it to retain, aggregate and use for R&D and/or Commercialization purposes in accordance with the license terms or by written authorization.

Employee: A person employed by Verisk directly or indirectly (i.e. contractor, consultant, part-time worker, intern, trainee, etc.) for wages or salary.

Employee Relations: The relationship between and among peer-to-peer employees and employer-to-employee. Verisk strives to provide a fair, equal and safe working environment for all employees.

Employee Safety: The process of protecting employees from injury or illness in the workplace, environmental risk, serious conflict or harm.

Ethical: The principle of what is perceived to be acceptable or unacceptable behavior as set forth in Verisk's Code of Conduct.

In Good Faith: Honesty or sincerity of intention

Interested Parties: Individuals with a need-to-know regarding information concerning an alleged case.

Internal Controls: Mechanisms, rules, and procedures implemented by Verisk to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.

Investigation: A careful search or examination, whether formal or informal, intended to develop a factual record.

Physical Security - The protection of people, property, and assets from physical actions that could cause damage or loss.

Report a Concern Review Committee: A cross-functional committee including leadership from functions such as Enterprise Risk Management, Internal Audit, Legal, Information Security, Corporate Compliance Governance, Human Resources and Global Protection Services. The committee meets quarterly to review hotline administration, operations and case trends.

Reporter: An individual who provides information about a concern affecting Verisk business, reputation, employees and/or other such entities directly or indirectly relating to Verisk business.

Owner; Questions or Concerns

Verisk's General Counsel is the Owner of this Whistleblower Policy. Should you have questions or concerns about this Policy, please contact CorporateComplianceGovernance@verisk.com.

Reviews; Updates

The Policy Owner will annually review and update this Whistleblower Policy, in consultation with all relevant stakeholders and the Report a Concern Review Committee. The Policy Owner will also update it on an ongoing basis as needed to reflect emerging legal requirements or accurately capture business practices. The Corporate Compliance Governance Department will have oversight for reviewing all changes and the coordination of obtaining required approvals.

Monitoring; Violations

Compliance Monitoring & Oversight (CM&O) will verify compliance with this Whistleblower Policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Policy Owner. Any suspected violations of this Whistleblower Policy or its supporting standards may be reported to the Verisk Report a Concern Hotline either:

- online at https://verisk.ethicspoint.com; or
- by telephone, to one of your country helpline numbers available at https://verisk.ethicspoint.com;

Remember to choose the correct category when reporting to assist in routing your report to the relevant team.

Remediation

Where applicable, substantiated reports will require a remediation plan, developed by the case investigation team, which may include members from Enterprise Risk Management Legal, Internal Audit, Compliance, Human Resources, Privacy, Information Security and/or Global Protection Services, depending on the subject of the report. The case investigation team will be responsible for overseeing and executing the remediation plan.

Communication and Training

All Verisk employees shall receive a copy of the Whistleblower Policy at time of hire and complete the required Commitments Month and/or new hire training to gain awareness and knowledge of the Whistleblower program.

Disciplinary Action

Any Verisk employee who is found to have violated this Whistleblower Policy may be subject to disciplinary actions up to and including termination of their employment contract.

Exceptions

Business unit specific policies may outline location specific legal and regulatory Whistleblower requirements. Such requirements should supersede the requirements set forth in this policy. Exceptions to this policy will be handled on a case-by-case basis at the discretion and approval of the General Counsel and the Report a Concern Review Committee.

References

Employee Covenants
Code of Conduct

Appendices

Whistleblower Policy – Verisk PL Policy Addendum
Whistleblower Policy – Verisk PL Policy Addendum Frequently Asked Questions (“FAQs”)

Revision History

Version	Date	Section(s)	Change Made By	Change Description
1.0	11/2021	All	N/A	Initial release
2.0	1/2025	All	Policy Owner; Corporate Compliance Governance	Reformatting; updating of department names; procedure clarifications; creation of Polish Verisk PL Policy to address additional specific requirements per Polish whistleblower law.