SiriusPoint Whistleblower Policy

Whistleblower Policy

Contents

Whistleblower Policy

Purpose and Objective

The purpose of the SiriusPoint Ltd. (the "Group") **Whistleblower Policy** (the "Policy") is to establish procedures for the submission of complaints or concerns regarding financial statement disclosures, accounting, internal accounting controls, auditing matters or violations of the Group's Code of Business Conduct and Ethics (the "Code").

This Policy is intended to comply with the requirements of Section 301 of the Sarbanes-Oxley Act, Section 922 of the Dodd-Frank Act of 2010 and the New York Stock Exchange's listing standards.

SiriusPoint Ltd. ("SiriusPoint" or, the "Company") is committed to a culture of ethics, integrity and strives to ensure compliance with applicable laws and regulations. In line with this commitment and our Code of Business Conduct and Ethics (the "Code"), SiriusPoint has established channels for reporting incidents without fear of retaliation. The purpose of this Whistleblower Policy (the "Policy") is to encourage disclosure of any wrongdoing that may adversely impact the Company, the Company's policyholders, employees, or the communities in which the Company does business. This Policy also outlines the individuals responsible for receiving reports and initiating the investigative procedures in addition to safeguarding any individual who files an incident report.

Scope

This Policy applies to all employees, consultants, officers, and directors of the Company. Additional local Whistleblowing procedures or guidelines may be applicable and should be read in conjunction with this Policy, please refer to the Related Policies section below for any local Whistleblowing procedures. Appropriate subjects to report under this Policy include but are not limited to financial improprieties, accounting or audit matters, ethical violations, or other similar illegal or improper practices by any employee, agent or representative of the Company, such as:

(a)Fraud.
(b)Theft.
(c)Embezzlement.
(d)Bribery or kickbacks.
(e)Misuse of the Company's assets.
(f)Undisclosed conflicts of interest.
(g)Harassment, discrimination or retaliation.

This Policy is applicable to the worldwide operations of the Company. The Company and its wholly-owned subsidiaries, unless otherwise indicated, must comply with all applicable laws and regulations of their respective domicile, which may be different from that of SiriusPoint Ltd. For Sirius International Insurance Corporation (SINT, Sirius International Managing Agency Limited (SIMA) and their respective wholly-owned subsidiaries, the intent and spirit of this Policy shall apply to their respective operations SINT and SIMA

shall prepare a supplemental Guideline to be adopted by respective CEO outlining exceptions and deviations from this Policy

Types of Incidents to be Reported

Incidents that may be reported include, but are not limited to:

- Breaches of SiriusPoint policies or procedures, including our Code;
- Failure to comply with laws or regulations;
- Miscarriage of justice;
- Criminal offenses;
- Fraud;
- Embezzlement;
- Bribery or Kickbacks;
- Misuse of Company Assets;
- Behavior that harms or is likely to harm the reputation or financial well-being of the Company;
- Damage to the environment;
- Putting the health or safety of individuals in danger;
- Any other unethical, illegal or questionable practices; or
- Deliberate concealment of any of the points noted above.

When not to use the Whistleblowing Channel

The whistleblowing channel should not be used for issues that would normally be reported to Human Resources or the Claims Department.

If you are uncertain and do not know what falls in scope under this policy, please contact Compliance for guidance.

The Group strictly prohibits retaliation of any kind by any Group officer, director, associate or agent against any employee, associate or other interested party who in good faith reports or participates in an investigation of reported complaints of questionable or illicit conduct.

Reporting Channels

Employees, consultants, officers and directors or third parties can report incidents through various channels such as by mail, email, or our Ethics Helpline. The reporting individual should provide names, dates, places and other details sufficient to facilitate an effective investigation of the incident reported. If the reporting individual would like to discuss any matter with the Audit Committee, he or she should so indicate in the submission and include a telephone number at which they can be reached, should the Audit Committee deem such communication is appropriate. Reports received will be assessed and

investigated initially by the Legal, Regulatory and Compliance team. The Head of Internal Audit will assess and investigate any reports implicating the Chief Legal Officer or any member of the Legal, Regulatory or Compliance team. Other stakeholders may be notified and involved as required to follow up on necessary actions.

<table>
<tr><td colspan="2">Via Mail (openly or anonymously)</td></tr>
<tr><td>Internally</td><td>Externally</td></tr>
<tr><td>By delivery to the Chief Legal Officer of the Group, or Chairman of the Audit Committee in an envelope labelled with a legend such as: “Attention Audit Committee. Submitted pursuant to the Group’s Whistleblower Policy.”</td><td>Through our third-party hotline service provider. Please refer to our website or the home page of our Intranet for contact details and further information.</td></tr>
<tr><td colspan="2">The reporting individual should provide names, dates, places and other details sufficient to facilitate an effective investigation of the matter reported. If the reporting individual would like to discuss any matter with the Audit Committee, he or she should so indicate in the submission and include a telephone number at which he or she can be reached, should the Audit Committee deem such communication is appropriate.</td></tr>
<tr><td colspan="2">Via Email
To the Group Compliance Mailbox: group.compliance@siriuspt.com</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Via Hotline
To the Navex EthicsPoint Hotline:
https://secure.ethicspoint.com/domain/media/en/gui/48395/index.html</td></tr>
</table>

Via Telephone From Bermuda	971-371-7843
Via Telephone From Belgium	0-800-100-10
Via Telephone From Canada	855-866-3866

Via Telephone From Sweden	020-79-8729
Via Telephone From Switzerland	0-800-890011
Via Telephone From the UK	0808-234-2941
Via Telephone From the United States of America	1-855-866-3866

Investigations

1. Depending upon the nature and severity of the incident received under this Policy, the Chief Legal Officer may notify the Chairman of the Audit Committee. No person who is the subject of an incident will receive such a notification.

2. The Chief Legal Officer, to the extent the Chief Legal Officer deems necessary or appropriate, will undertake a preliminary investigation on behalf of the Audit Committee to determine if the information can be substantiated. Upon receiving the results of the preliminary investigation, the Chairman of the Audit Committee will determine if any further action is required to follow up on the reported incident.

3. The Chairman of the Audit Committee has the power to take any appropriate action including, among other things to: (1) refer the matter to the full Audit Committee; (2) refer the matter to the full Board of Directors; (3) further investigate the matter; (4) direct that a further internal investigation be conducted; or (5) retain outside counsel, accountants or other third-party advisors to investigate.

4. The Legal, Regulatory and Compliance team will maintain a log of all incidents received, tracking their receipt, investigation, and resolution. A quarterly report will be provided by the Head of Internal Audit to the Audit Committee for all incidents received or confirming no incidents received.

5. All information disclosed during any investigation will remain confidential, except as necessary to conduct, conclude, and, if appropriate, prosecute the investigation. In the case of any anonymous complaint, a person who reports an incident may not be informed of the results of an investigation.

6. All employees, consultants, officers and directors (including members of management) have a duty to promptly cooperate and provide accurate information in connection with any investigation of reports of incidents.

7. Prompt and appropriate corrective action will be taken when and as warranted. The specific action taken in any case depends on the nature and gravity of the conduct or circumstances reported, and the facts proven by investigation. Any persons responsible for any misconduct, or those failing to cooperate or who provide false information during an investigation, may be subject to disciplinary action, up to and including termination.

Non-Retaliation Policy

SiriusPoint prohibits retaliation against any individual who has made a report in good faith. Individuals who report incidents should ensure that, to the best of their knowledge, the information provided is accurate and made in good faith. Any employee who retaliates against someone who has reported a violation of good faith may be subject to disciplinary action, up and including termination of employment. Any claims of acts of retaliation should be submitted to the Legal, Regulatory and Compliance Team or the Chairman of the Audit Committee to initiate a confidential investigation.

Anyone knowingly providing inaccurate or misleading information may result in the possibility of civil or criminal liability.

Confidentiality and Protection

Reports made via the SiriusPoint Ethics Helpline may contain confidential, sensitive or personal information. The confidentiality and security of reports and records will be protected by restricting access to members of the Audit Committee, the Legal, Regulatory and Compliance Team, Internal Audit and any individuals involved in the investigation of a reported incident. Access to reports and records may be granted to other parties at the discretion of the Audit Committee.

Retention of Records

The Legal, Regulatory and Compliance Department will retain records in accordance with applicable record retention requirements.

Review and Modifications

The Policy will be reviewed on an annual basis. The Audit Committee or the Board of Directors can modify this Policy at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with applicable legal requirements or to accommodate Company organizational changes.

Communication and Training

All employees have access to this policy via the SiriusPoint intranet. Training on our Code and how to report concerns is provided annually to all employees.

Related Policies

SiriusPoint Ltd. Code of Business Conduct and Ethics

Board of Directors Communication Policy

Whistleblowing Guideline