Whistle Blower – Internal Investigations Policy

Scope and Purpose

LightRiver, Inc. (the "Company") strives to conduct itself according to the highest standards of lawful and ethical conduct and to comply with all federal and state laws and regulations. The Company strictly prohibits and will not tolerate violations of its policies or the law in any form, including discrimination, harassment, insider trading, fraud, corruption, bribery, and failure to comply with laws and regulations. The Company treats allegations of violation of the law and its policies seriously and will take all steps necessary to investigate and address allegations of misconduct.

As part of its commitment to ethical and lawful behavior, the Company encourages employees and other Company stakeholders to report any concerns about violations of law or Company policy and seek guidance from Company resources on legal or policy questions. In addition, from time to time, the Company may also become aware of or involved with government inquiries, investigations, or other legal proceedings. Such reports or inquiries may present a need for the Company to investigate its own operations to:

- Gather information to determine facts and circumstances
- Accurately respond to requests for information
- Defend against allegations of Company wrongdoing
- Take appropriate action with respect to individual wrongdoing
- Determine needed changes to current operations to better comply with the law

This Internal Investigation Policy ("Policy")

- Describes how employees and other Company stakeholders can report concerns and ask questions about ethical and legal compliance matters
- Describes how employee reports and questions are handled
- Explains the specific requirements and prohibitions associated with internal investigations
- Sets out the Company's expectations of all employees in connection with internal investigations

Applicability

This Policy is applicable to all the Company's operations worldwide. This Policy applies to all the Company's directors, officers and employees. This Policy also applies to the Company's agents, consultants, joint venture partners and any other third-party representatives who have conducted business on behalf of the Company.

Definitions

For this policy, the following terms are defined as follows:

1. **Communication** includes:
    - Written and oral communications
    - Electronic communications
    - Physical gestures, such as nods
    - A customer's actions, such as transferring documents
2. **Attorney-Client Privilege** refers to a legal privilege that protects confidential communications between an attorney and a client from disclosure to third parties. Although company employees are not clients, the attorney-client privilege includes

communications between Company legal counsel and Company employees that are made for the purpose of obtaining or providing legal advice. The privilege belongs solely to the company.

3. **Attorney Work Product** means documents and tangible things that are prepared in anticipation of litigation by or for the client. The work product protection can extend to work products created by individuals who are not attorneys, including company employees, if created at the direction of attorneys, by agents of attorneys, or under the supervision of attorneys. This privilege protects these materials from discovery by opposing counsel and, like the attorney-client privilege, belong to the Company, not individual employees.
4. **Confidential Information** means information that may cause harm to the Company, its customers, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available. Damage may be to an individual's privacy, the Company's marketplace position or that of its customers, legal or regulatory liabilities.
5. **Witness** refers to individuals, including Company employees, who may have knowledge related to an internal investigation.
6. **Data** includes:
    - Electronically stored information (ESI) including its metadata, found on computer hard drives and other media. ESI may exist as word processing documents, spreadsheets, emails, text messages, recordings of telephone or video calls or conferences, social media content, data generated and stored by devices connected to the Internet of Things (IoT), and communications generated and stored in workplace collaboration tools (WCTs) (such as Slack, Microsoft Teams, or Google Meet) and ephemeral messaging applications (such as Snapchat, Confide, Telegram, or Wickr).
    - Hardcopy and original documents

Reporting Concerns and Asking Questions

Employees who wish to report a concern or ask a question about Company policies or legal issues may do so by contacting the HR Department or engage our third-party reporting source Insperity at (866) 715-3552.

Retaliation

Retaliation is strictly prohibited. The Company will not retaliate against (and will not tolerate retaliation against) any employee or other stakeholder who in good faith (a) reports a suspected violation of law or Company policy, (b) asks a question regarding ethical or legal obligations, or (c) participates in an internal investigation as a witness or otherwise.

Grounds for Internal Investigations

Internal investigations may be conducted for a variety of reasons. An investigation may be compulsory, while others may be discretionary and prompted by allegations regarding misconduct. The decision to engage in an internal investigation may be a matter of policy, regulation, or left to the discretion of the Company's board of directors or the individuals to whom the board has delegated the decision.

Investigation Management

Internal Investigations will be primarily overseen by an Investigation Supervisor ("Supervisor") who will be named by the CEO, Board of Directors or a special committee created by the Board of Directors in response to the allegations necessitating the internal investigation. The CEO, Board of Directors or special committee may see fit, depending on the circumstances of the investigation, to engage outside legal counsel to act as Supervisor of an internal investigation.

The role of the Supervisor in an investigation is to:

- Determine the initial scope and focus of the investigation
- Determine the facts of the allegations or events giving rise to the investigation
- Coordinate the investigation, including necessary adjustments to the scope, focus and duration
- Communicate with the appropriate corporate representative(s) during the investigation
- Identify and seek direction regarding any potential conflicts of interest that may be presented during the investigation
- Examine Company's reporting obligations and determine whether a report is required
- Determine whether and to what extent the results will be reported, and if so, to whom and in what format
- Design a corrective action plan, if needed, to address investigation findings
- Assist in the development of stronger controls, policies, or compliance processes to address deficiencies identified during the investigation

Employee Cooperation

The Company appreciates and depends on the cooperation of its employees and agents when conducting internal investigations. Company employees are required to cooperate with Company investigations. Employee refusal to cooperate in a company investigation may result in discipline measures up to and including termination. Investigations may be conducted by designated Company representatives and the Company's legal counsel. Company employees may be asked for information related to an investigation by the Company's legal counsel. Company legal counsel represents the Company, not any individual employee.

Communications

Privileged Communications

The Company has a strong interest in maintaining the confidentiality of certain internal communications, including communications protected from disclosure to third-parties due to the attorney-client privilege and attorney work product doctrine. Communications with Company legal counsel may be protected by the attorney-client privilege, but the privilege belongs to the Company and not any individual employee. This means that only the Company may waive the attorney-client privilege, not the individual employee. The Company relies on its employees and agents to be mindful of confidentiality, privilege, and discretion when it comes to documentation and communications related to business activities.

Company employees and agents should be instructed by counsel as to the limits and requirements of the attorney-client and work product protections when creating documents and communicating in writing, including by email and text. All privileged documentation and communications should be clearly labeled, although the presence of a label or legend on a document or communications will not by itself protect the contents.

External Communications
Unless specifically authorized by the [CEO/Supervisor], Company employees must not publicly disseminate Company information about an internal investigation. Only those employees or agents of the Company that are specifically authorized by the Company to speak on its behalf may communicate with government agencies on behalf of the Company. This Policy does not preclude employees from speaking to government agencies in their own, individual capacities.

Outside Sources

Outside Counsel
The CEO and the Board of Directors may engage outside legal counsel to advise on matters related to internal investigations. Independent outside counsel must be retained to manage all investigations involving the CEO or any members of the Board of Directors.

- **Criteria:** Outside counsel engaged to advise on or manage an internal investigation should be highly qualified, experienced in the area and/or with the government agency involved, and should have no relationship with any entity or person that would pose a conflict of interest in the counsel's representation of the Company.
- **Individual Counsel Representation:** Employees of the Company have a right to their own legal representation.

Outside Consultants
The Supervisor may engage outside consultants to perform tasks essential to facilitate a thorough and complete investigation.

Outside consultants may include:

- Forensic accountants
- Forensic document collection vendors and examiners
- Outside Auditors
- Subject matter experts
- Legal Counsel

Consultants must report directly to the Supervisor and shall maintain all investigation related documentation and information in such a manner as to preserve privilege under the attorney work product doctrine.

Data Preservation and Collection

Preservation
Preservation of relevant hardcopy documents, electronic data, and other physical material is an immediate concern upon indication of a potential issue that may trigger an internal investigation, government investigation, or litigation. Preservation requires immediate issuance of an appropriately tailored preservation notice to all persons who may have relevant materials. Steps must be taken to ensure that potentially relevant material is preserved, including the imaging of employee hard drives, if necessary. The Company will take immediate steps to preserve all data related to an investigation, including relevant inactive data residing on back-up tapes, archival media, cloud-based storage, or elsewhere. Employees are prohibited from deleting or destroying any data relevant to an investigation. Prior to collection, the Supervisor will work with the Company's IT Resources to develop a plan for identifying, collecting, and preserving electronic information in a forensically sound manner that preserves all relevant data, including metadata.

Employees may be interviewed to determine whether they possess data relevant to the investigation, where it is stored, and how best to collect it.

Documentation
A record must be kept of all preservation efforts made by the Company. The record will include copies of all notices, memos, and communications related to the collection and preservation of data.

Collection
Data collection and preservation should begin as soon as the scope of the investigation has been reasonably determined. If relevant data may be destroyed in the normal course of business, efforts to preserve the data should start immediately, even if the scope of an investigation has not yet been determined. When in doubt, preserve. The Company may collect potentially relevant evidence (including hardcopy documents, data, and other tangible items) from any source that the company owns, possesses, or controls. Data may be collected from all mediums owned by the company. Collection may also occur from employee personal devices used in the furtherance of Company business in accordance with any Company policies relating to use of employee-owned devices for work purposes. If an employee-owned device such as a cell phone is used for business purposes; the Company has the right to collect data from the employee-owned device.

Information from sources owned by the Company belong to the Company. The Company cannot guarantee that employee personal emails, documents, text messages, or other data will not be collected, reviewed, or produced to a third party, including government agencies. In certain instances, as determined by the Supervisor, data collection may occur without notice to employees.

Witness Interviews
The Company may interview current and former employees as a part of an internal investigation.

Interviews will be conducted by the Supervisor or the Supervisor's delegate. The interviews may be conducted in-person or by video or telephone. It is the Company's expectation that parties involved in interviews be truthful and provide complete answers to interview questions. Retaliation for mere participation in an interview is strictly prohibited. All witnesses will be treated with respect and provided information regarding:

- Interviewer's role
- The reason for the interview
- Attorney-client privilege and its relevancy to the interview, where applicable
- Potential disclosure of information discovered during the investigation to any third party, including government agencies

Investigation Report
Investigation Report:

1. The Supervisor will develop an Investigation Report detailing the investigation, its findings, and recommendations for final review by the Supervisor
2. The Supervisor has full authority over the Investigation Report
3. The nature, scope, and content of any presentation of findings of the Investigation Report shall be determined by the Supervisor.

Government Reports

Required Disclosures: Information regarding misconduct, culpable individuals, violations, and other information discovered during an internal investigation that are required by law or by contractual agreement to be disclosed to the government, the public, or other parties must be properly disclosed within the legally specified time frame.

Voluntary Disclosures: Information regarding misconduct, culpable individuals, violations, or other information discovered during an internal investigation which is not required by law to be disclosed to the government, the public, or other parties may nevertheless be disclosed at the discretion of the Board of Directors.

Corrective Action

Employee misconduct, as well as deficiencies in controls, policies, and standards identified by the investigation, must be analyzed and corrective action must be taken to address them. Disciplinary action warranted by the findings of an internal investigation will be administered according to Company policy.

Cease Misconduct: Any illegal acts, criminal conduct, or other misconduct identified during the internal investigation will be immediately stopped.

Development of Corrective Action Plan: The Supervisor will develop a Corrective Action Plan (CAP) to address each specific deficiency, violation of law, or element of misconduct found during an internal investigation. The Supervisor will work with the Company executive responsible for compliance within the department(s) relevant to the investigation findings, and HR Manager to implement the CAP. A CAP may include employee discipline in accordance with Company policy. The CAP will include an implementation schedule and protocols for verifying that the corrective actions are effective in remediating the deficiencies or misconduct.

Development of Strong Compliance Controls: The Supervisor will work with the Company executive responsible for compliance within the department[s] relevant to the investigation findings and HR Manager to ensure that new or revised policies and controls are implemented to address compliance concerns found during an internal investigation.

Policy Compliance

Company employees, agents, and other third-party representatives must understand and comply with the provisions of this Policy. Violations of this Policy by Company employees are subject to disciplinary action, up to and including dismissal. Third-party representatives, including outside legal counsel, who violate this Policy may be subject to termination of all commercial relationships with the Company. Any Company employee, agent, or other third-party representative who suspects that this Policy may have been violated must immediately make a report through the reporting process outlined above. Any Company employee who, in good faith, reports suspected legal, ethical, or Policy violations will not suffer any adverse consequence for doing so.

Amendments and Waivers

The Company reserves the right to interpret, administer, change, modify, or rescind this policy at any time, with or without notice, to the maximum extent permitted by law. No statement or representation by a supervisor or manager or any other employee, whether oral or written, can supplement or modify this policy. Changes will only be valid if approved in writing by the Company's CEO or other official to whom such authority has been delegated in writing.

No delay or failure by the Company to enforce any work policy or rule will constitute a waiver of the Company's right to do so in the future.

Administration of this Policy

The Chief Financial Officer is responsible for the administration of this Policy. All employees are responsible for consulting and complying with the most current version of this Policy. If you have any questions regarding this Policy or concerning the scope or delegation of authority, please contact the HR Department.