

WHISTLEBLOWER POLICY

Purpose

Cloud Software Group Holdings, Inc., its subsidiaries and affiliates (collectively, “Cloud Software Group”), is committed to being a leader in business ethics and regulatory compliance, while maintaining an atmosphere of open communication and trust between employees and management. For those reasons, Cloud Software Group maintains a workplace where employees who reasonably believe that they are aware of conduct in violation of our legal duties or policies can raise those concerns free of any harassment, discrimination or retaliation. Therefore, we encourage those employees to report those concerns as set forth in this Whistleblower Policy (“Policy”).

1. Reporting and Investigation

If you have reason to believe that you have become aware of any conduct covered by this Policy, you must immediately report those facts as set forth below. Examples of reportable actions include, but are not limited to, any indication of fraud, misappropriation of company resources, substantial variation in our financial reporting methodology from prior practice or from generally accepted accounting principles, conduct that is not honest and ethical, conflicts of interest, potential violations of governmental rules and regulations or our Code of Business Conduct and Ethics, the falsification, concealment or inappropriate destruction of corporate or financial records, discrimination, harassment, or retaliation.

Any report may be made anonymously, at your option, and must be made in one of the following ways:

- By contacting your manager;
- By contacting our General Counsel at alex.kolar@cloud.com; or
- By accessing the Integrity HelpLine at [EthicsPoint - Cloud Software Group](#), which will process your report and forward it to appropriate Cloud Software Group personnel for investigation.

For employees located outside the United States, local law may limit the types of reports that can be made through the Integrity HelpLine at [EthicsPoint - Cloud Software Group](#). In those instances, employees should make their reports by contacting their managers or the or Contact Person to determine the appropriate process for making a report.

Cloud Software Group

Investigations at Cloud Software Group may be conducted or directed by members of Cloud Software Group including, but not limited to the legal and security teams. And, in appropriate circumstances Cloud Software Group may involve law enforcement in a matter being investigated.

In addition to the methods described above, employees may make reports by mail to the Board of Directors at:

Cloud Software Group
Board of Directors c/o General Counsel
851 West Cypress Creek Road, Fort Lauderdale
Florida 33309 U.S.A

If you believe your manager or any Contact Person is involved in the matters raised in your report, you should make your report through the Integrity HelpLine at [EthicsPoint - Cloud Software Group](#). Any manager receiving a report will, consistent with local law, forward that report to our General Counsel by using one of the reporting methods. However, whether your report is submitted through EthicsPoint or through any other means, your report will not be sent to any implicated person.

Regardless of which reporting method you choose, please include in your report a discussion of the following items: (i) a description of the matter or irregularity, (ii) the period of time during which you observed the matter or irregularity, and (iii) any steps that you have taken to investigate the matter or irregularity, including reporting it to your manager and his/her reaction. The report may include, at your option, your contact information in the event that additional information is needed.

All complaints made pursuant to this Policy will be taken seriously and will be promptly and thoroughly reviewed. In all instances, Cloud Software Group retains the right to determine when circumstances warrant an investigation and, in conformity with the Policy and applicable laws and regulations, the appropriate investigative process to be employed. All information disclosed during the course of the investigation will remain confidential, except as necessary to conduct the investigation and take any remedial action in accordance with Cloud Software Group policies and applicable law. Although Cloud Software Group will do its best to keep confidential not only your report but also the identity of the people being investigated, Cloud Software Group cannot assure you that the identity of all parties will remain confidential.

All employees and managers have a duty to cooperate in the investigation of reports of any conduct covered by this Policy. Employees will be subject to disciplinary action, including the termination of their employment, if they fail to cooperate in an investigation or deliberately provide false information during an investigation. In addition, destroying, altering or tampering with documents related to an on-going internal or external investigation is prohibited by Cloud Software Group's Code of Business Conduct and Ethics, and may be a violation of law.

Cloud Software Group aims to complete investigations as timely as possible, however, we are not able to immediately determine how long Cloud Software Group will need to complete an investigation. We recommend that all involved in the matter focus their efforts on meeting the expectations of their position, while keeping their investigator apprised of any new issues that arise. If an employee believes they need additional support during an investigation, they should let their investigator know so that Cloud Software Group can determine whether and how it can assist. Cloud Software Group may take immediate or interim actions to protect the complainant, other employees, or Cloud Software Group's systems or assets. For example, in matters involving employees and/or Cloud Software Group systems, Cloud Software Group may consider temporarily placing one or more employees on administrative leave or suspending access to certain systems or facilities. This may be done at any stage in an investigation, including early in an investigation, as a measure of caution and does not necessarily indicate that Cloud Software Group has made any finding or determination.

If, at the conclusion of its investigation, Cloud Software Group determines that a violation of our legal duties or policies has occurred, we will take remedial action commensurate with the severity of the offense. That action may include disciplinary action against the accused party, up to and including termination. The specific action taken in any particular case depends on the nature and gravity of the conduct or circumstances reported and the quality of the information provided. Reasonable and necessary steps will also be taken to prevent any further violations of law or policy.

2. Discrimination, Retaliation or Harassment

Any employee reporting concerns under this Policy has a lawful right to raise those concerns without fear of discrimination, retaliation, or harassment. As a result, Cloud Software Group strictly prohibits any discrimination, retaliation or harassment against any person who reports conduct in violation of our legal duties or policies based on the person's reasonable belief that such misconduct occurred. The prohibited forms of intimidation or retaliation include, but are not limited to, discharge, demotion,

suspension, threats, harassment, or any other manner of discrimination with respect to an employee's terms or conditions of employment.

Cloud Software Group also strictly prohibits any discrimination, retaliation or harassment against any person who participates in an investigation of such complaints, including, but not limited to:

- By providing information and otherwise assisting in investigations conducted by (A) a federal regulatory agency, (B) a member or committee of the United States Congress or (C) any of our officers or employees, any member or committee of our Board of Directors or any agent or representative acting on their behalf; or
- By filing, testifying at, participating in or otherwise assisting a proceeding filed or about to be filed relating to allegations of fraud or other misconduct.

If you later believe that you have been subject to discrimination, retaliation, or harassment for having made a report under this Policy, you must immediately report all relevant facts to your manager and/or any Contact Person. If you have reason to believe that all of those persons are involved in the matter you wish to report, then you should report those facts to the Board of Directors. It is imperative that you bring those matters to our attention promptly, so that any concern of discrimination, retaliation, or harassment can be investigated and addressed promptly and appropriately.

Any complaint that any managers, supervisors or employees are involved in discrimination, retaliation or harassment related to the reporting or investigation of conduct in violation of our legal duties or policies will be promptly and thoroughly investigated in accordance with our investigation procedures. If a complaint of discrimination, retaliation or harassment is substantiated, appropriate disciplinary action, up to and including discharge, will be taken.

3. Additional Enforcement Information

In addition to our internal complaint procedure, employees should also be aware that certain law enforcement agencies are authorized to review legal compliance, including reviewing questionable accounting or auditing matters, or potentially fraudulent reports of financial information.

Before issues or behavior rise to that level, employees are encouraged to report questionable accounting or auditing matters, suspicion of fraudulent financial information, or discrimination, retaliation or harassment related to such reports. Nothing

in this Policy is intended to prevent an employee from reporting information to the appropriate agency when the employee has reasonable cause to believe that the violation of a federal or state statute or regulation has occurred.

Cloud Software Group's policies and practices have been developed as a guide to our legal and ethical responsibilities to achieve and maintain the highest business standards. Conduct that violates our policies will be viewed as unacceptable under the terms of employment at Cloud Software Group. Certain violations of our policies and practices could even subject Cloud Software Group and/or the individual employees involved to civil and/or criminal penalties.

4. Modification

Cloud Software Group can modify this Policy unilaterally at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with state and federal regulations and/or to accommodate organizational changes within the company.

© CLOUD SOFTWARE GROUP 2022

Revision	Prepared by	Date Prepared	Comments/Notes
1.0	J Ingram	19/10/2022	
Effective Date	Reviewed by	Date Reviewed	Comments/Notes
Owner	Approved by	Date Approved	Comments/Notes