

LEGALZOOM.COM, INC.

OPEN DOOR POLICY FOR REPORTING
COMPLAINTS REGARDING ACCOUNTING, AUDITING, FRAUD, FINANCIAL AND DATA SECURITY
MATTERS (“WHISTLEBLOWER POLICY”)

STATEMENT OF POLICY

LegalZoom and its subsidiaries (the “*Company*”) is committed to providing a workplace conducive to open discussion of our business practices and is committed to complying with the laws and regulations to which we are subject. Accordingly, the Company will not tolerate conduct that is in violation of such laws and regulations. Each Company employee is encouraged to promptly report good faith complaints or concerns regarding accounting, auditing, internal accounting controls, fraud or violations of law, regulation or policy that could impact the Company’s financial statements (“*Compliance Matters*”), as well as good faith complaints regarding data security (“*Data Security Matters*”), in accordance with the provisions of this whistleblower policy (this “*Policy*”). Employees who file reports or provide information without a good faith, reasonable belief in the truth and accuracy of such information are not protected by this Policy and may be subject to disciplinary action. Any other third party, such as vendors, collaborators, partners, stockholders or competitors, also may report, under the procedures provided in this Policy, a good faith complaint regarding Compliance Matters or Data Security Matters. To facilitate the reporting of complaints regarding Compliance Matters, the audit committee of our Board of Directors (the “*Audit Committee*”) has established procedures for (i) the receipt, retention and treatment of complaints regarding Compliance Matters and (ii) the confidential, anonymous submission by Company employees of concerns regarding Compliance Matters.

This Policy is a supplement to the Company’s Code of Business Conduct and Ethics (the “*Code*”) and should be read in conjunction with the Code.

SCOPE OF COMPLIANCE MATTERS COVERED BY THIS POLICY

This Policy covers complaints relating to Compliance Matters and Data Security Matters, including, without limitation, the following types of conduct:

- fraud, deliberate error or gross negligence or recklessness in the preparation, evaluation, review or audit of any financial statement or other disclosure of the Company;
- fraud, deliberate error or gross negligence or recklessness in the recording and maintaining of financial records or other disclosures of the Company;
- deficiencies in, or noncompliance with, the Company’s internal accounting controls;
- misrepresentation or false statement to management, regulators, the outside auditors or others or by a senior officer, accountant or other employee regarding a matter contained in the financial records, financial reports or audit reports or with respect to other disclosures of the Company;
- deviation from full and fair reporting of the Company’s results or financial condition;
- unauthorized access to data, information, or systems, or other data security incidents;

- other violations of law, regulation or Company policy; or
- such other matters as may be referred by the Audit Committee to the Compliance Officer designated in the Code (the “*Compliance Officer*”).

POLICY OF NON-RETALIATION

It is the Company’s policy to comply with all applicable laws that protect our employees against unlawful discrimination or retaliation by us or our agents as a result of their lawfully reporting information regarding, or their participation in, investigations involving Compliance Matters. If any employee believes he or she has been subjected to any harassment, threat, demotion, discharge, discrimination or retaliation by the Company or its agents for reporting complaints regarding Compliance Matters in accordance with this Policy, he or she may file a complaint with the Compliance Officer, chair of the Audit Committee or the Company’s human resources department. If it is determined that an employee has experienced any improper employment action in violation of this Policy, we endeavor to promptly take appropriate corrective action.

Nothing contained in this Policy or the Code limits or otherwise prohibits any employee from communicating with, filing a charge or complaint, or otherwise participating in any investigation or proceeding with any federal, state or local governmental agency or commission, including providing documents or other information, without notice to the Company.

COMPLIANCE OFFICER

The Compliance Officer is responsible for receiving, reviewing and investigating complaints under this Policy (under the direction and oversight of the Audit Committee), and may be reached at complianceofficer@legalzoom.com. If an employee has a complaint regarding a Compliance Matter or Data Security Matter, he or she should report such matter to the Compliance Officer. If the suspected violation involves the Compliance Officer, the employee should instead report the suspected violation to the chair of the Audit Committee.

ANONYMOUS REPORTING OF COMPLAINTS

We have also established a procedure under which complaints regarding Compliance Matters or Data Security Matters may be reported anonymously. Employees and third parties may submit reports to our Compliance Hotline using one of the methods listed below, and will be given the option of identifying themselves or remaining completely anonymous:

- **Website:** www.lighthouse-services.com/legalzoom
- **Anonymous Reporting App:**
 - Keyword: legalzoom
 - Detailed instructions available [here](#).
- **Toll-Free Telephone:**
 - **English speaking USA and Canada: (855) 222-1644**
 - Spanish speaking USA and Canada: (800) 216-1288

- French speaking Canada: 855-725-0002
 - Spanish speaking Mexico: 01-800-681-5340
 - All other countries: (800) 603-2869 (must dial country access code first click here for access codes and dialing instructions)
- **E-mail:** reports@lighthouse-services.com (must include company name with report)
 - **Fax:** (215) 689-3885 (must include company name with report)

Employees and third parties should make every effort to report their concerns using one or more of the methods specified above. The complaint procedure is specifically designed so that employees have a mechanism that allows the employee to bypass a supervisor he or she believes is engaged in prohibited conduct under this Policy. Anonymous reports should be factual, instead of speculative or conclusory, and should contain as much specific information as possible to allow the Compliance Officer and other persons investigating the report to adequately assess the nature, extent and urgency of the investigation.

POLICY FOR RECEIVING AND INVESTIGATING COMPLAINTS

Upon receipt of a complaint, the Compliance Officer, who may consult with internal or external counsel, will determine whether the information alleged in the complaint pertains to a Compliance Matter or Data Security Matter.

The Audit Committee shall be notified promptly of all complaints determined to pertain to a Compliance Matter and shall determine the planned course of action with respect to the complaint, including determining that an adequate basis exists for commencing an investigation. Reports regarding Compliance Matters related to the Company's foreign subsidiaries will be forwarded to the appropriate personnel at the foreign subsidiary. The Compliance Officer will then appoint one or more internal and/or external investigators to promptly and fully investigate each viable claim under the direction and oversight of the Audit Committee or such other persons as the Audit Committee determines to be appropriate under the circumstances. The Compliance Officer will confidentially inform the reporting person (if his or her identity is known) that the complaint has been received and provide him or her with the name of, and contact information for, the investigator assigned to the claim.

Complaints determined to pertain to a Data Security Matter will be promptly reviewed by the Senior Director of Privacy and Compliance and/or the Director of Information Security, who may at the direction of the Compliance Officer, direct and oversee any investigation of such reports. As appropriate, they may delegate the oversight and investigation of such reports to other LegalZoom personnel, such as the Chief Technology Officer or other employees appointed by the Compliance Officer, or to outside advisors.

Confidentiality of the employee submitting the complaint will be maintained to the fullest extent possible, consistent with the need to conduct an adequate investigation. In the course of any investigation, the Company may find it necessary to share information with others on a "need to know" basis. If the investigation confirms that a violation has occurred, the Company will promptly take appropriate corrective action with respect to the persons involved, including discipline up to and including termination, and, in appropriate circumstances, referral to governmental authorities, and will also take appropriate steps to correct and remedy any violation.

RETENTION OF COMPLAINTS

The Compliance Officer will maintain a log of all complaints, tracking their receipt, investigation and resolution, and shall prepare a periodic summary report thereof for each member of the Audit Committee. Each member of the Audit Committee and, at the discretion of the Compliance Officer, other personnel involved in the investigation of complaints, shall have access to the log. Copies of the log and all documents obtained or created in connection with any investigation will be maintained in accordance with our document retention policy.

Approved by the Audit Committee: March 7, 2022

Effective: March 7, 2022