WELLTOK, INC.

OPEN DOOR POLICY FOR REPORTING COMPLAINTS RELATING TO THE CODE OF BUSINESS CONDUCT AND ETHICS

As Adopted by the Board of Directors and Audit Committee on May 3, 2016

Statement of Policy

Welltok, Inc. ("***Welltok***" and together with its subsidiaries, the "***Company***") is committed to complying with all laws that govern our business, including those that govern our accounting and auditing practices and compliance with federal and state privacy and security requirements. We also encourage open discussion within the workplace of our business practices and will not tolerate conduct that is in violation of laws and our internal policies. If a Company employee has a good faith complaint regarding a possible violation of law or policy, including that with regard to accounting or auditing matters or compliance with applicable federal and state privacy and security requirements, we expect the employee to report the complaint promptly in accordance with this policy. Other third parties, such as consultants or vendors, also may report a good faith complaint regarding accounting or auditing matters in accordance with this policy.

The Audit Committee of our Board of Directors has established these procedures to facilitate the reporting of complaints. This policy is a supplement to our Code of Business Conduct and Ethics.

Scope of Matters Covered by Policy

This policy covers complaints relating to accounting matters, including the following:

- fraud, deliberate error or gross negligence or recklessness in the preparation, evaluation, review or audit of the financial statements of the Company;
- fraud, deliberate error or gross negligence or recklessness in the recording and maintaining of financial records of the Company;
- deficiencies in our internal accounting controls or noncompliance with them;
- misrepresentations or false statements to management, regulators, the outside auditors or others by a senior officer, accountant or other employee regarding a matter contained in the financial records, financial reports or audit reports of the Company; or
- deviation from full and fair reporting of our results or financial condition.

This policy also covers complaints relating to the Company's policies and practices designed to safeguard confidential information and compliance with federal and state privacy and security laws, including the following:

- Violations of federal and state privacy and security laws and regulations, including the Health Insurance Portability and Accountability Act ("***HIPAA***");
- The breach of unsecured Protected Health Information as defined under HIPAA; or
- Violations of the Company's policies and procedures designed to preserve the confidential information of the Company and its customers.

Policy of Non-Retaliation

The Company will not retaliate against any individual for filing a good-faith complaint regarding non-compliance with this policy. The Company will not retaliate against any individual participating in the investigation of any such complaint either. Finally, the Company will not permit any such retaliation by any manager or executive officer, or by any company with which we contract. If any employee believes he or she has been subjected to any such discrimination or retaliation, or the threat of it, they may file a complaint with our Chief Compliance Officer. We will take appropriate corrective action if an employee has experienced any improper employment action in violation of this policy.

Chief Compliance Officer

The Company's Chief Administrative Officer, Jim Sullivan, shall initially be the Company's Chief Compliance Officer and shall serve at the pleasure of the Board (Phone: 949-719-2203; email: jim.sullivan@welltok.com). The Chief Compliance Officer is responsible for receiving, reviewing and then investigating (under the direction and oversight of the Audit Committee) complaints under this policy. If an employee has a complaint covered by this policy, he or she should report such matter to the Chief Compliance Officer. If the suspected violation involves the Chief Compliance Officer, the employee should report the suspected violation to our Chief Executive Officer or any member of the Audit Committee.

Anonymous Reporting of Complaints

To the extent you are not comfortable reporting a suspected violation to our Chief Compliance Officer, we have also established a procedure under which complaints covered by this policy may be reported anonymously. Employees may anonymously report these concerns by either (i) leaving an anonymous message via a toll free telephone call at 844-591-0569; (ii) submitting an anonymous report to the EthicsPoint website at welltok.ethicspoint.com; or (iii) delivering the complaint anonymously via regular mail to Jim Sullivan, Chief Compliance Officer, at Welltok, Inc., 1675 Larimer Street, Suite 300, Denver, CO 80202.

Employees should make every effort to report their concerns either directly to the Chief Compliance Officer or by 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 Chief 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 Chief Compliance Officer will determine whether the information alleged in the complaint pertains to a subject covered under this policy. The Audit Committee Chairperson, on behalf of the Audit Committee, will be notified promptly of all complaints that pertain to an accounting or audit matter, and will determine the planned course of action for such complaints. Complaints regarding matters other than accounting or audit will be investigated by the Chief Compliance Officer or other appropriate person designated by the Chief Compliance Officer.

Initially, the Audit Committee Chairperson or the Chief Compliance Officer, as the case may be, will determine if there is an adequate basis for an investigation. If so, the Chief Compliance Officer will appoint one or more internal or external investigators to promptly and fully investigate the claim(s) under the direction and oversight of the Audit Committee. The Audit Committee may also appoint other persons to provide direction and oversight of the investigation. The Chief Compliance Officer will also confidentially inform the reporting person (if their identity is known) that the complaint was received and

whether an investigator has been assigned. If so, the reporting person will be given the name of the investigator and his or her contact information.

Confidentiality of the employee submitting the complaint will be maintained to the fullest extent possible consistent with the need to conduct an adequate investigation. The Company may find it necessary to share information on a “need to know” basis in the course of any investigation however.

If the investigation confirms that a violation has occurred, the Company will promptly take appropriate corrective action with respect to the persons involved. This may include discipline up to and including termination. Further, in appropriate circumstances, the matter may be referred to governmental authorities that may investigate and initiate civil or criminal proceedings. Of course, the Company will also take appropriate steps to correct and remedy any violation.

Retention of Complaints

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